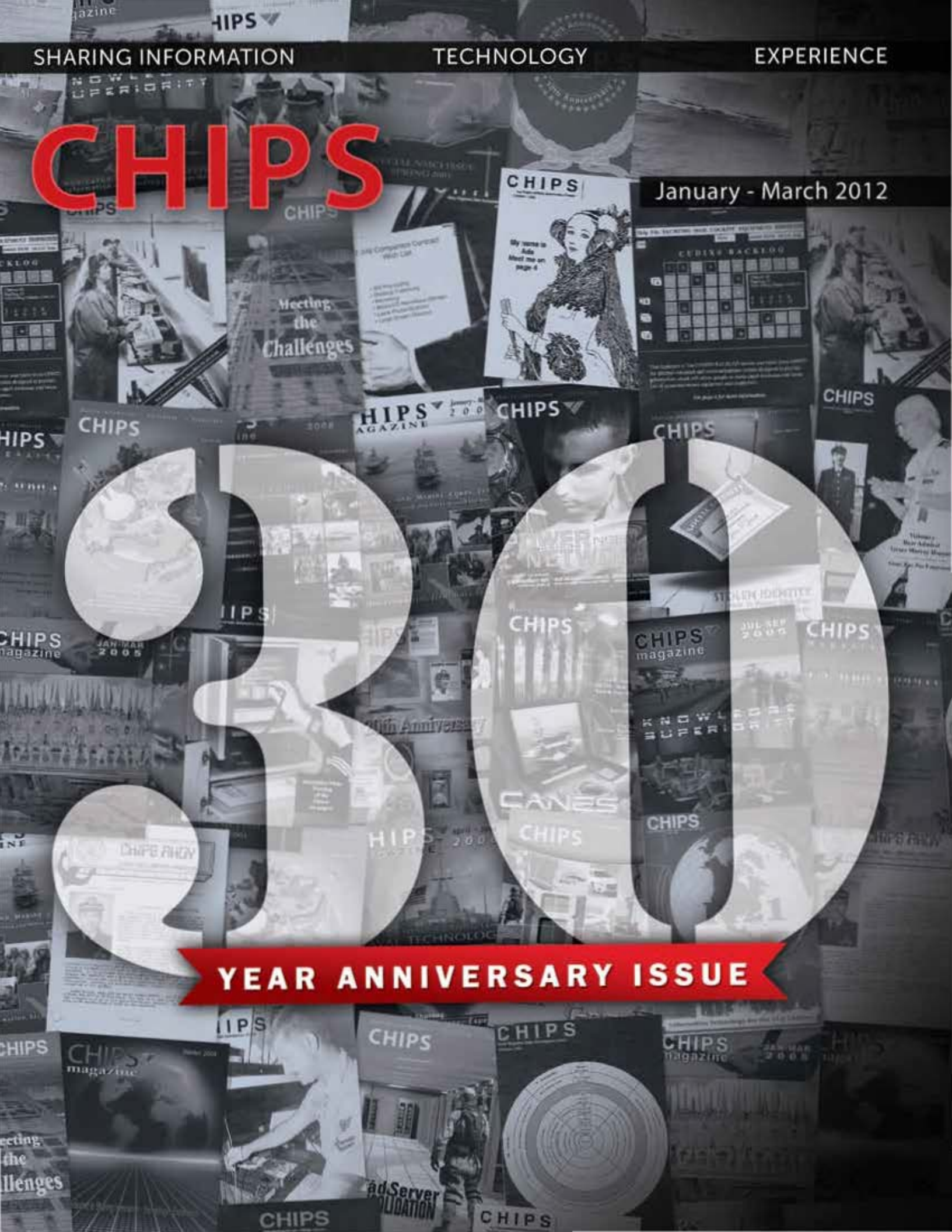
SHARING INFORMATION TECHNOLOGY EXPERIENCE

CHIPS

January - March 2012



CHIPS January – March 2012 | Vol. XXX Issue I

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO), the DoD Enterprise Software Initiative and the DON's ESI software product manager team at SPAWARSYSCEN Pacific. CHIPS (USPS 757-910) is published quarterly by SPAWARSYSCEN Atlantic, 1837 Morris St., Suite 3311, Norfolk, VA 23511. Periodical postage paid at Norfolk, VA and additional entry offices.

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SPAWARSYSCEN Atlantic, 1837 Morris St., Suite 3311, Norfolk, VA 23511-3432, or call (757) 443-1775; DSN 646. Email: chips@navy.mil; Web: www.doncio.navy.mil/chips.

ISSN 1047-9988; Web ISSN 2154-1779: www.doncio.navy.mil/chips.

POSTMASTER: Send changes to CHIPS, SPAWARSYSCEN Atlantic, 1837 Morris St. Suite 3311, Norfolk, VA 23511-3432.

Cover

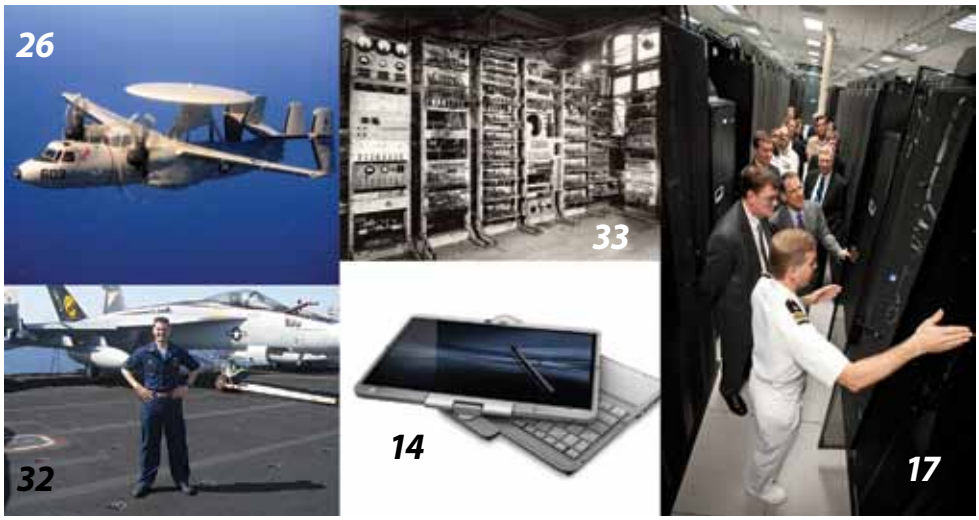
Marking 30 years as the Department of the Navy information technology magazine. Looking back, but more important, looking forward to another 30 years of technology achievements that secure the utmost safety and effectiveness of Sailors and Marines at the tip of the spear.

Interviews

Statement of Ownership, Management and Circulation
The U.S. Postal Service requires all publications to publish an annual statement of ownership, management and circulation.

Date	1 July 2011
Title of Publication	CHIPS
Title of Publisher	U.S. Navy
USPS Publication Number	ISSN 1047-9988
Editor	Sharon Anderson
Frequency of Issue	Quarterly
Owner	U.S. Navy
Total No. of Copies Printed	30,000
No. Copies Distributed	29,760
No. Copies Not Distributed	240
Total Copies Distributed and Not Distributed	30,000
Issue Date for Circulation	July-September 2011
Location of Office of Publication	SPAWARSYSCEN Atlantic CHIPS Magazine 1837 Morris St. Suite 3311 Norfolk, VA 23511-3432

Navigation



In Every Issue

Highlights

Please update your bookmark, the CHIPS website address has changed to www.doncio.navy.mil/chips.

Email CHIPS at chips@navy.mil.

From the DON CIO

From Around the Fleet and Program Offices

30 YEAR ANNIVERSARY ISSUE

Editor's Notebook – A Short History of CHIPS

Many times I am asked why the Department of the Navy's IT magazine is named "CHIPS." The CHIPS name represents the microchip. When CHIPS first began publication 30 years ago, desktop technology was just rolling out across the DON and Defense Department and the mighty microchip was the single most important technology breakthrough bringing computing power to individuals. It may seem hard to believe, but 30-plus years ago, only government agencies and large companies could afford the computing power that individuals now have at their fingertips.

If you can remember typing computer instructions at the MS-DOS "C Prompt" — you can appreciate just how far the DON has come in computing power and security with the advent of the Navy Marine Corps Intranet in 2000.

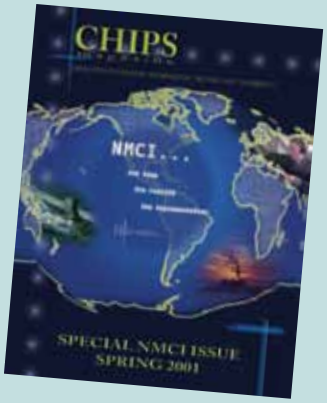
The first issue of CHIPS was published in 1982 by the Navy Regional Data Automation Center (NARDAC). It was distributed as a newsletter titled "Chips Ahoy." The Ahoy portion of the name was dropped later — for obvious reasons — even though we thought of the name first!

Chips Ahoy was electronically mailed to an incredibly small IT community of 2,500 Navy personnel, and it was the first electronic magazine delivered as an ASCII text edition mailed over the Defense Data Network (DDN) to 250 host administrators in 1987, preceding the World Wide Web by seven years.

From its inception, the CHIPS motto has been to "Share Information, Technology, Experience." Early editions of CHIPS featured instructions for such software applications as dBase and Harvard Graphics and user forums for government off-the-shelf software (GOTS) and the Ada programming language. From its humble beginnings, CHIPS provided all-important information about the DON IT Umbrella program of contracts for software applications and hardware to speed the deployment of desktop technology across the Navy and Defense departments at the best possible prices.

In April 1991, NARDAC merged with Naval Communication Area Master Station Atlantic to form the Naval Computer and Telecommunications Area Master Station Atlantic, and CHIPS was realigned under NCTAMS LANT. Another realignment followed in February 2000, with CHIPS moving under the Space and Naval Warfare Systems Center Charleston (Charleston was changed to Atlantic in 2008).

In 1999, the DON Chief Information Officer and SPAWAR entered into a memorandum of understanding to jointly sponsor CHIPS. Through the changes, there are many constants: CHIPS still reports the all-important information about IT enterprise contracts, but now through the DoD Enterprise Software Initiative; Moore's Law, which states that the chip gets smaller about every 18 months, still holds true, and CHIPS continues to deliver on its founding motto.



Now in its 30th year of publication, CHIPS comes full circle back to its digital roots. This edition will be the last CHIPS that will be printed and mailed. In the spirit of the DoD and DON cost-savings and efficiencies initiatives, CHIPS will be published in digital format only — please continue to enjoy CHIPS online at www.doncio.navy.mil/CHIPS. We will keep to our quarterly publishing schedule so please continue to write and email your articles to chips@navy.mil.

Many thanks to CHIPS' writers and longtime subscribers for your loyalty over the last 30 years.

Sharon Anderson

A MESSAGE FROM THE

DON CIO

Happy New Year!

The actual cost of printing is between 6 cents and 13 cents per page, or $600 to $1,300 per year per employee…

This year, the Department of the Navy will build on the efforts of 2011 as we continue on our difficult but necessary journey to transform the way the department manages its business information technology. Finding ways to become more effective in how we acquire and operate IT will lead to decreased costs and ensure we hit the target of reducing the IT budget by 25 percent by 2017.

There is no question that this is a monumental task in an agency as big as the Department of the Navy with more than 800,000 personnel around the world. But the good news is we have already made great strides finding efficiencies and reducing costs by consolidating data centers (see "Consolidating Data Centers Key to Cutting IT Spending" on page 6), streamlining processes (see related memos at www.doncio.navy.mil/efficiencies), "killing" obsolete applications, optimizing systems, leveraging enterprise contracts (see "New DON Mobile Contracts and Tools Drive Savings" on page 24), and acting in a more centralized manner. Additionally, stringent approval processes have been put in place to achieve better visibility and to control spending. As a result, we have gained a lot of knowledge about the information technology environment and the true cost of IT.

In addition to these efforts, priorities for 2012 include further enhancing transparency and tracking IT dollars by establishing metrics and reporting processes, and implementing the process to approve information technology purchases exceeding a certain threshold. We will also be working closely with the Department of Defense and Defense Information Systems Agency to develop and implement effective and cost-efficient DoD enterprise IT systems.

Further, we will work to improve the security of our IT systems by developing a risk/cost analysis, improving DON Federal Information Security Management Act scores and establishing the first DON policy on communications security accountability. Many changes are occurring, but rest assured current capabilities will not be sacrificed simply to cut costs.

While my staff and the different integrated product teams, task forces and working groups involved in these important efficiencies efforts do the analysis, write the policies and implement the necessary changes, you too can do your part to help the department reduce its spending. One way is to reduce the amount of printing you do personally and organizationally. According to a Citigroup Environmental Defense study, the actual cost of printing is between 6 cents and 13 cents per page, or $600 to $1,300 per year per employee. Now multiply that by the number of men and women working for the DON, and you begin to see how even small changes in the way we do business can make a positive impact. I encourage you, as I have my staff, to reevaluate what you consider necessary to print. A lot of what is printed, according to the study, is not intended to be printed in the first place.

I have directed my office to reduce the amount of printing we do. I've encouraged electronic review of documents rather than printing hard copies, we've stopped printing schedules for our DON IT conferences, and CHIPS magazine will cease to print hard copies and become completely digital this year.

This makes sense in a digital and increasingly federal budget-constrained age. These are things great and small that we as a department can do to cut costs and meet the challenge to decrease business IT spending by $2 billion over the next five years. We are all in this together, and in the end it will truly make this department a stronger, more effective Navy-Marine Corps team.

There is a lot of activity to support this effort and my staff is working to keep department personnel informed of key decisions, changes in processes and success stories by publicizing this information using the DON CIO website, email alerts, CHIPS magazine and other communication tools. One way to ensure you receive the latest DON IT news is to sign up for the DON CIO website's RSS feed so that the news comes to you.

Finally, I'd like to congratulate Sharon Anderson, senior editor of CHIPS magazine, and the many contributors to the Department of the Navy's IT magazine on its 30th anniversary. The first issue of CHIPS was published in 1982 as a newsletter and was mailed to 2,500 Navy personnel.

Today, CHIPS is read by more than 2 million people composed of DoD, federal, state and local government agencies; allies and coalition partners; academia; and industry partners. Its founding motto: "Dedicated to Sharing Information, Technology and Experience," still holds true today as the magazine continues to meet the needs of CHIPS' diverse readership by providing informative interviews and features. CHIPS

Terry Halvorsen

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
www.doncio.navy.mil

Consolidating Data Centers Key to Cutting IT Spending

By Michele Buisch

To continue supporting the operational forces stationed around the world, protecting the nation and providing humanitarian assistance during these fiscally constrained times, the Department of the Navy (DON) is seeking opportunities to increase IT efficiencies while cutting business spending. A primary focus of this effort is data center consolidation, which is essential to reducing the IT budget by 25 percent during the next five years.

To date, there are approximately 150 DON data centers that support delivery of computing capabilities to users. Over the years, the proliferation of Navy and Marine Corps data centers has led to a complex, duplicative and costly network structure.

The goal of the department's data center consolidation initiative is to virtualize and reduce the number of software applications used and select a small number of enterprise data centers for retention and close the remainder. Consolidation of the data centers and reducing the number of applications department-wide will reduce network complexity and the overall cost of purchasing, manpower support, testing, certification, operation and maintenance, while meeting security and operational requirements. Efficiencies are gained by consistently delivering common computing capabilities as services to users.

One such enterprise data center that will be retained is the Space and Naval Warfare (SPAWAR) Systems Center Atlantic data center, which opened this past fall on Joint Base Charleston-Weapons Station. The cutting-edge facility uses new technologies and optimizes systems, while providing enhanced capabilities and requiring less manpower.

"This data center … provides the Navy a state-of-the-art platform that gets us another step closer to information domination. Within this data center we will be able to support significantly more work with fewer personnel without sacrificing service or capability," Capt. Mark Glover, commanding officer of SPAWAR Systems Center Atlantic, said during the ribbon-cutting ceremony. "In cooperation and combination with data centers in New Orleans and San Diego, this building represents a capability and a capacity to be exactly what the Navy needs at a time when the Navy needs it."

Additionally, the 20,220-square-foot building, which is one-third the size of its predecessor, is environmentally friendly, designed to the U.S. Green Building Council's Leadership in Environmental and Energy Design (LEED) standards.

"Not only is this data center efficient, it's green — that is another big piece of what we want to do. We need to protect the environment and the resources that we have. This data center will help us do that," said Mr. Terry Halvorsen, DON Chief Information Officer, who also attended the center's ribbon-cutting ceremony. "The Navy and Marine Corps team is the best value we get in defense. We need to protect that. Efforts like this help."

Data center consolidation is part of a larger effort within the department to find efficiencies and cut spending in business IT. It was also mandated by President Obama in February 2010 with the launch of the Federal Data Center Consolidation Initiative (FDCCI), which instructs federal CIOs to inventory their agency data centers and develop consolidation plans for implementation in fiscal year 2012 budget submissions. The goal, as with the DON's consolidation efforts, is to reduce costs, enhance the department's IT security posture, apply best practices and promote energy efficiencies. The federal goal is to reduce the number of data centers, which has grown from 432 in 1998 to 2,094 in 2010, by at least 800 over five years, according to the "25 Point Implementation Plan to Reform Federal Information Technology Management," published in December 2010.

How many and which DON data centers will be retained is still under review; however, the strategy will be to consolidate all legacy data centers into the following three data center environments:

- **SPAWAR:** Three locations (San Diego, Charleston and New Orleans);
- **Marine Corps:** One location (Kansas City, Mo.); and
- **Navy Marine Corps Intranet (NMCI):** A number of existing DON-owned NMCI locations that will be selected for retention following further review.

The DON CIO established a moratorium on data center investments, according to a July 20, 2011 memo, "DON Data Center Consolidation Policy Guidance," which states that before purchasing additional data center capacity, the Navy and Marine Corps must determine that existing capacity is insufficient to meet the requirement and that it is less cost-effective to expand into existing SPAWAR, NMCI or Marine Corps enterprise or regional data centers.

Progress is already being made. The Navy established a Navy data center consolidation task force to assess the current state and close as many data centers as feasible during the next five years. To date, the Navy has closed 13 data centers and plans to close 22 more during the next fiscal year and at least 58 by FY17 in an effort to realize the Navy's target of $1.4 billion in net savings for the department from data center consolidation.

The Marine Corps is evaluating local computing centers and isolated server hosting facilities for opportunities to consolidate, with plans to complete regionalization of IT infrastructure assets into its four enterprise and seven regional data centers. The Marine Corps Enterprise IT Services (MCEITS) Center in Kansas City, Mo., will be the centerpiece of the Marine Corps data center consolidation strategy.

The demand for IT efficiencies will continue as the federal budget shrinks. Through data center consolidation and the development of modern enterprise facilities, the department will increase its IT efficiencies, reduce spending and increase its operational effectiveness. CHIPS

Michele Buisch provides communications support to the Department of the Navy Chief Information Officer.

Q&A with Rear Adm. Joseph Mulloy – Deputy Assistant Secretary of the Navy for Budget; Director, Fiscal Management Division OPNAV (N82)

A discussion about IT efficiencies

Rear Adm. Joseph Mulloy assumed responsibilities as Deputy Assistant Secretary of the Navy for Budget (FMB)/ Director, Fiscal Management Division, OPNAV (N82) in October 2009.

The Office of the Assistant Secretary of the Navy, Financial Management and Comptroller produces numerous products and provides many services of interest to the public. This includes the annual President's Budget submission for the Department of the Navy and detailed justification materials, aligning resources with the priorities of the Secretary of Defense, Secretary of the Navy, the Chief of Naval Operations and the Commandant of the Marine Corps.

These are summarized in the "Highlights of the Department of the Navy Budget," an annual publication. FMB provides guidance concerning the organization and functioning of comptroller organizations throughout the Navy and Marine Corps. This includes oversight and reduction of the information systems needed to achieve the objective of producing timely, accurate and audit-ready financial information.

Due to the national economic crisis and by direction of the Secretary of Defense, the Department of the Navy is conducting strategic reviews and efficiency efforts across the department. In December 2010, the Under Secretary of the Navy, Robert O. Work, issued a memorandum, "Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment," directing the DON Chief Information Officer, Mr. Terry Halvorsen, to find efficiencies and cost savings in how the department delivers IT/cyberspace capabilities and information resources management. Mr. Work targeted a 25 percent reduction in business IT spending.

The Chief of Naval Operations, Adm. Jonathan W. Greenert, and Under Secretary Work have said that every program in the DON is under scrutiny to achieve the department's objectives for cost savings and efficiency. CHIPS asked Rear Adm. Mulloy to discuss the role his office is playing in helping the department meet its share of the anticipated reduction in the DoD budget.

Rear Adm. Joseph Mulloy

CHIPS spoke with Rear Adm. Mulloy Nov. 22, 2011.

CHIPS: Before we go to my questions, do you have any opening comments?

Mulloy: The DON's IT infrastructure is the backbone of our ability to manage resources, operate the supply chain, improve the infrastructure and communicate effectively. We cannot function without robust IT to enhance the capability of our workforce and continue productivity improvements. IT is more than just business architecture; it's more than just communications. IT truly is an enabler for fleet operations, fleet execution, and it is actually part of our weapons systems.

In addition, the IT budget is a partnership between FMB and the DON CIO, which supports the strategic vision and framework for the DON information environment. FMB asks hard questions to ensure IT requests are justified and aligned with the DON's ongoing IT efficiency efforts. In these challenging times, we have to learn to do more with less, and I have no doubt we will succeed and come out leaner and meaner while continuing to provide first-rate support to our warfighters.

CHIPS: In December 2010, Mr. Work directed the DON CIO, Mr. Terry Halvorsen, to closely examine the department's business IT spending to achieve a 25 percent reduction in costs over five years. Secretary Work said that identifying and managing IT costs are difficult because IT is a critical infrastructure that cuts across every program in the DON. How is your office helping to track and identify where IT dollars are spent?

Mulloy: As part of the Department of the Navy budget, no single budget line exists for business IT. However, there are business rules for program and budget IT business resources within the framework of OMB Circular A-11 and the Clinger-Cohen Act. Requirements are identified as part of the Program Objective Memorandum (POM) process, which includes input from combatant commanders to ensure we meet our responsibility to train, equip and deploy naval forces.

These requirements are validated by the Chief of Naval Operations and Commandant of the Marine Corps, as well as functional area managers. A goal of the current IT budget process is to increase granularity. Using a bottom-up budget approach, the Naval Information Technology Exhibits/Standard Reporting System (NITE/STAR) captures details for the approximately $7 billion annual DON IT budget. The DON uses the same methodology and systems to report actual spending for business IT and National Security Systems (NSS) to the Office of the Secretary of Defense (OSD) and the Office of Management and Budget (OMB).

IT budgets are developed through an integrated process, supporting the DON CIO and the Office of the Budget in the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), to validate the completeness of IT budgets, ensuring compliance at each level of management oversight. The DON is committed to IT efficiencies and managing costs. We are continuing to do so by identifying how much we are spending on IT, strengthening the DON's IT gov-

ernance and reducing DON business IT costs.

CHIPS: An area that's getting a lot of attention across the federal government is data center consolidation. What are your thoughts on that?

Mulloy: Data center consolidation provides an opportunity for efficiencies and cost savings, and it is one area where we are making great strides. The Navy has already closed 13 data centers with plans to close 22 more in FY12 and 58 by FY17.

By consolidating data centers, we realize savings in several areas: decreased maintenance costs to sustain data centers, decreased energy costs to operate data centers, and decreased hardware and software costs. We have new policy on data storage and data centers that establishes a moratorium on all investment of increased data storage capacity. Before purchasing additional data center capacity, we must first determine that existing capacity is insufficient to meet the need.

"By consolidating data centers, we realize savings in several areas: decreased maintenance costs to sustain data centers, decreased energy costs to operate data centers, and decreased hardware and software costs."

We must also determine that it is not more cost effective to expand capacity into one of the existing NMCI (Navy Marine Corps Intranet), SPAWAR (Space and Naval Warfare Systems Command) or Marine Corps enterprise or regional data centers. Together, these initiatives support our end state — an efficient, streamlined and integrated data center portfolio supporting warfighting and business requirements at minimal cost.

CHIPS: How are IT requirements reported? How are you working to standardize reporting methods in the DON?

Mulloy: IT requirements are reported through: (1) the normal budget process by appropriation, and (2) the Information Technology (IT)/National Security Systems (NSS) budget in the OSD single data repository for the IT/NSS Budget, which has more than 1,170 categories.

The DON has consistent guidance for assessing program costs and is following the lead of the Federal CIO in the '25 Point Implementation Plan to Reform Federal Information Technology Management' to plan, develop, manage, operate and govern IT toward the goals that produce efficient and effective IT.

"The DON has consistent guidance for assessing program costs and is following the lead of the Federal CIO in the '25 Point Implementation Plan to Reform Federal Information Technology Management' to plan, develop, manage, operate and govern IT toward the goals that produce efficient and effective IT."

CHIPS: What additional information can you provide about changes to the Standard Accounting and Reporting System (STARS) that support greater audit ability within the department's financial system?

Mulloy: The major change to STARS resulting from audit readiness assessments allows end-to-end traceability of financial transactions. STARS-FL execution codes are mapped to United States Standard General Ledger (USSGL) codes, but the historical mapping has not been consistent. By updating STARS, we will ensure future STARS-FL transactions are accurately and reliably mapped to USSGL codes. We're also researching historical transactions back to FY 2007 to align with current structured query language (USSQL) mapping.

CHIPS: In his memorandum of 19 July 2011, the DON CIO established a policy requiring review and service level approval by the Information Technology Expenditure Approval Authority (ITEAA) of any IT expenditure greater than $1 million (life cycle). Is this threshold still valid, or has that threshold been adjusted since the 25 percent or $2 billion reduction in IT savings was targeted?

Mulloy: The $1 million threshold for review and approval of IT expenditures by Navy and Marine Corps ITEAAs remains in effect. It is our expectation that this approval process will identify and control spending, contribute to a smaller DON IT 'footprint,' and help to ensure that items purchased will smoothly integrate into our future architecture without generating unusual support costs.

"The $1 million threshold for review and approval of IT expenditures by Navy and Marine Corps ITEAAs remains in effect. It is our expectation that this approval process will identify and control spending, contribute to a smaller DON IT 'footprint,' and help to ensure that items purchased will smoothly integrate into our future architecture without generating unusual support costs."

CHIPS: When you briefed the fiscal year 2012 budget roll-out at the Pentagon, Feb. 14, 2011, you said that the department is working to meet the requirements of the law for federal agencies to file audit-ready financial statements. How can the department's business IT systems, such as Enterprise Resource Planning, help meet this requirement?

Mulloy: To achieve financial audit ability, we have to strengthen the controls in our end-to-end business processes, such as civilian and military pay, and contractor pay. IT systems are integral components of these business processes, and all of our business systems must be surveyed for audit readiness on our way to financial audit ability.

This includes major accounting systems like the Standard Accounting and Report-

ing System and Navy Enterprise Resource Planning. Navy ERP has an embedded array of strong internal controls over Navy business processes, which will increase the likelihood that the financial data, which rolls up into our financial statements, is accurate and reliable. In addition, there is an ongoing working group to ensure that business processes (including the way we employ our business systems) are standardized among all of our major commands.

Fewer variations in the way we do business will result in greater efficiency through streamlining, with fewer internal controls necessary. This will also increase the accuracy and reliability of financial data. Incidentally, we have moved our repair parts inventory management under Navy ERP, and this has resulted in efficiencies, which will improve asset reporting on our financial statements.

CHIPS: Based on your past experiences with IT and budgets, what are your thoughts as we move forward on IT efficiencies for the DON?

Mulloy: There is a balancing act with IT requirements. In our development of POM 13, the Secretary of the Navy has had us build on the Secretary of Defense's efficiency initiatives from the FY 2012 President's Budget and continue the identification and implementation of efficiencies to enable increased investment in warfighting capabilities.

The DON continues to assess options that allow for the necessary balance between sustainment of operations, preservation of fleet readiness, and support of our Sailors, Marines and their families, based on fiscal reality and force structure requirements. As part of this process, we are reviewing all areas of our budget plans for savings. Nothing is off the table. We are facing different challenges with the current fiscal environment and in order to find savings and plan for the future, we are identifying savings through efficiencies.

As you mentioned, the Under Secretary tasked the DON CIO to achieve a 25 percent reduction in costs over five years. This was later defined to the requirement to find $2 billion in business IT savings. As a result, some of our processes have been updated to better manage our spending. Now, approval is required before spending over a certain threshold, the business case for IT requirements must be shown, and IT investments must be assessed for efficiency and effectiveness. This focus on IT efficiencies forces us to spend from a strategic, enterprise-wide perspective while saving money.

CHIPS: Do you have any closing remarks?

Mulloy: I think it's a very exciting time. Major budget changes are upon us, and IT will play a large part. The focus of the CNO indicates, and it's clear from the Under Secretary and the DON CIO, that IT is a crucial element of our focus as we manage these changes. The new 10th Fleet commander [Vice Adm. Michael S. Rogers] is a former JCS J2 (Joint Chiefs of Staff director for intelligence) and a cryptologist.

We're in a business IT world but we recognize IT is also part of defending and maintaining ourselves in a cyber world. Like great navigators, I think the Navy has properly put our focus on the world ahead of us. We are going to completely integrate these areas of DON CIO, 10th Fleet, N2/N6 (Deputy Chief of Naval Operations for Information Dominance/ Director of Naval Intelligence and Deputy CIO – Navy) and SPAWAR to make the department run leaner but also realize that the networks can be viewed as a weapons platform.

Everything on it [the network] can either be helping us or potentially be used to hurt us. For example, a weakness in LOGCOP, our logistics common operating picture, could be an in-road to our networks and our overall IT capabilities — we need to defend all of it, and we need to enable all of it. CHIPS

Links

Office of the Assistant Secretary of the Navy Financial Management and Comptroller: www.finance.hq.navy.mil/FMC/.

Office of the Assistant Secretary of the Navy Financial Management and Comptroller Office of Financial Operations: www.fmo.navy.mil/.

IT Efficiency & Effectiveness Policy

DON IT Efficiencies Policy

DON Information Technology/ Cyberspace Efficiency Initiatives and Realignment from the Under Secretary of the Navy (12/2010): www.doncio.navy.mil/PolicyView.aspx?ID=2061.

DON Information Technology/Cyberspace Efficiency Initiatives and Realignment from the DON CIO (12/2010): www.doncio.navy.mil/PolicyView.aspx?ID=2073.

DON Enterprise Information Technology Standard Business Case Analysis Template (4/2011): www.doncio.navy.mil/PolicyView.aspx?ID=2211.

Required Use of DON Enterprise Information Technology Standard Business Case Analysis Template (6/2011): www.doncio.navy.mil/PolicyView.aspx?ID=2506.

DON Information Technology Expenditure Approval Authorities (7/2011): www.doncio.navy.mil/PolicyView.aspx?ID=2508.

DON Data Center Consolidation Policy Guidance (7/2011): www.doncio.navy.mil/PolicyView.aspx?ID=2504.

Efficiency and Effectiveness Review of DON IT Systems from the Under Secretary of the Navy (9/2011): www.doncio.navy.mil/PolicyView.aspx?ID=2835.

DON Secretariat Information Technology Expenditure Approval Authority from the Under Secretary of the Navy (9/2011): www.doncio.navy.mil/PolicyView.aspx?ID=2834.

Federal CIO IT Efficiencies Policy

Federal Cloud Computing Strategy: www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.

Federal Data Center Consolidation Initiative: www.cio.gov/documents/Federal-Data-Center-Consolidation-Initiative-02-26-2010.pdf.

25 Point Implementation Plan to Reform Federal Information Technology Management: www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf.

Navy Information Technology Procurement Approval and Oversight

From the Office of the Deputy Chief of Naval Operations for Information Dominance
Vice Adm. Kendall L. Card

At the direction of the Chief of Naval Operations, and in coordination with the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RD&A), the Deputy Chief of Naval Operations for Information Dominance released a naval message in November, NAVADMIN 346/11, "Information Technology Procurement Approval and Oversight," to inject increased rigor into the Navy's objective to reduce IT costs and enhance operational efficiencies.

To achieve clarity, visibility and discipline in IT spending and procurement across the Navy, the existing approval process requires modification. The current process will be consolidated in a single Navy command under the centralized management of the Space and Naval Warfare Systems Command (SPAWAR).

The process modification will ensure effective and efficient expenditure of funding to acquire information technology capabilities (materiel classified as hardware, software or services); prevent duplicative investments; provide visibility on all Navy IT-related expenditures; and ultimately achieve strategic sourcing on IT procurement.

As defined in the Clinger-Cohen Act of 1996, IT encompasses any equipment, interconnected system, subsystem, service (including support service) or related resource used to access, retrieve, transport, process, analyze, and/or display non-tactical, business-related, or business process-related data or information. This includes all afloat and ashore IT, including hull, mechanical, and electrical systems (HM&E). This definition excludes weapon systems, but includes IT which supports weapon system program management and oversight.

Other items excluded from this definition are IT resources that are physically part of, and essential in real time to the mission performance of a weapons or command, control, communications, computer, intelligence, surveillance, reconnaissance (C4ISR) system. IT assets are shown in Figure 1.

Requirements

The revised policy applies to the IT procurement activities of all Navy commands and organizations, ashore and afloat, unless otherwise excepted by the provisions of the NAVADMIN: all IT procurement requests for non-weapon or non-C4ISR system related IT materiel and IT support services, regardless of whether the funding is reported in the IT budget, resourced with Navy appropriated and/or non-appropriated funds, must be processed, reviewed and approved using an information technology procurement request (ITPR) smart form. ITPRs less than $500,000 will be approved by the Echelon II command information officer (CIO). ITPRs for more than $500,000 will be forwarded by the requesting Echelon II to SPAWAR for approval.

All requests for IT, regardless of dollar amount, will be entered into an ITPR smart form and documented prior to purchase. Procurement actions for IT may not be initiated prior to ITPR approval in accordance with the NAVADMIN. ITPR smart forms with instructions will be made available by the DON Deputy Chief Information Officer – Navy (DDCIO-N) to all Echelon II CIOs for distribution to their respective Echelon III and IV users.

The ITPR smart form will be completed by requesting commands and then forwarded via email to their respective Echelon II CIO for processing.

All requests below $500,000 may be approved by the Echelon II CIO and documented. Echelon II CIOs must forward approved requests to SPAWAR for tracking within five (5) working days of granting approval. All requests greater than $500,000 will flow to SPAWAR for approval.

Requests for software must be submitted to the Echelon II CIO for approval by the appropriate functional area lead prior to procurement approval.

Requests for IT support services must include (attached to the ITPR smart form) a copy of the contract statement of work and any other supporting documentation for the services to be provided. The documentation must clearly define all IT-related tasks to include, but not limited to, procurement, development, installation, maintenance or modification of software, hardware or systems.

Requests for handheld wireless (commercially supported) communication devices (i.e., cell phones and BlackBerrys) and their services must be purchased via a Naval Supply Systems Command Fleet Logistics Center San Diego (NAVSUP FLC San Diego, formerly known as Fleet Industrial Supply Center San Diego) contract.

All ITPRs for handheld wireless devices through FLC San Diego must include a contract number. (For information, go to: https://www.navsup.navy.mil/navsup/ourteam/navsupgls/prod_serv/contracting/market_mgt.)

The FLC San Diego contract is not required for OCONUS units.

Responsibilities

Requests for non-tactical radios shall include the specific make and model information, spectrum assignment and waveform type, and will be reviewed and approved by the enterprise services functional area manager (FAM).

The DDCIO-N: (1) will ensure all software requests have been reviewed by the

To achieve clarity, visibility and discipline in IT spending and procurement across the Navy, the existing approval process requires modification. The current process will be consolidated in a single Navy command under the centralized management of the Space and Naval Warfare Systems Command (SPAWAR).

appropriate FAM leads and registered with a favorable disposition in the DON Application and Database Management System (DADMS); (2) coordinate with SPAWAR for periodic reviews of the IT approval process and IT procurement data analysis; and (3) codify the contents of the NAVADMIN in a formal OPNAV instruction by the end of fiscal year 2012.

SPAWAR will: (1) oversee and approve requests for hardware, software and services required to support Navy information systems and network infrastructure; (2) ensure requests for computers, servers and peripherals comply with DON criteria; (3) with the concurrence of the Naval Strategic Sourcing Working Committee (SSWC), identify existing contract vehicles and, as appropriate, establish and manage purchasing vehicles for IT on behalf of acquisition programs, operating forces and the supporting establishment; publish and update information regarding available contract vehicles for IT and enterprise licensing agreements for software; and (4) collect data on all IT procurement approvals and provide periodic reports to the DDCIO-N.

Navy budget submitting offices (BSO) will incorporate and reference the policy contained in NAVADMIN 346/11 in local regulations and standard operating procedures.

Comptrollers will support the ITPR process to ensure proper allocation and resourcing of approved IT.

Command information officers: (1) will ensure IT procurement requests are submitted via ITPR smart form; (2) review and approve or disapprove ITPRs under $500,000 that are not required to be submitted to higher authority under the requirements of NAVADMIN 346/11; (3) submit IT procurement requests exceeding $500,000 to SPAWAR for approval; and (4) maintain an ITPR history file and submit to higher authority when directed.

Functional area managers will review the potential impact of the requested IT procurement on additions to the respective functional area portfolio and recommend approval or disapproval to the Echelon II CIO.

The Bureau of Medicine and Surgery IT procurement requests are not required to use ITPR. However, Navy medicine support afloat will require ITPRs. CHIPS

To view NAVADMIN R 152325Z NOV 11, "Information Technology Procurement Approval and Oversight," go to: www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2011/NAV11346.txt.

To view Commander SPAWAR issued naval message R 012023Z DEC 11 ZYB, "Information Technology Acquisition Approval Process (ITAAP)," go to: www.public.navy.mil/spawar/Press/Pages/IT_PROCUREMENT_APPROVAL_AND_OVERSIGHT.aspx.

IT Assets

IT assets include, but are not limited to:

- Computer workstations/desktops
- Servers
- Computer processing units
- Mainframes
- Peripherals (i.e., displays, mouse, keyboard, speakers, Web cams, smart card reader, multimedia switch, media converters, fax, etc.)
- Storage devices
- Laptops
- Personal digital assistants
- Handheld Internet access devices, tablets, etc.
- Cell or smart phones and air cards
- Wi-Fi access points
- Routers
- Switches
- Firewalls, inline network encryption, intrusion detection systems, information assurance/computer network defense devices
- Cabinets, chassis and equipment racks
- Power supplies and surge suppressors
- Power over Ethernet devices
- Printers
- Copiers
- Scanners
- Bar code readers
- Video teleconference (VTC) equipment (to include televisions and flat screens)
- Software applications (commercial off-the-shelf (COTS) or government off-the-shelf GOTS), including common applications (i.e., Microsoft Office, Adobe Reader, Symantec, etc.), databases (i.e., Oracle, DB2, SQL, etc.) and operating systems (i.e., Windows, Linux, OS X, VMware, etc.)
- Portals and websites
- Collaboration, knowledge and records management tools
- Telephones, telephone switches including Voice-over-Internet Protocol (VOIP) and Internet Protocol telephony and call managers
- Circuits
- IT services
- Training and education associated with IT assets

The following are examples of IT not included in the provisions of the new policy:

- Weapons systems (platform IT);
- IT expendables (paper, ink, toner, compact disc and digital video disc, media, etc.);
- IT support services required for development, installation, maintenance, modification, or procurement and/or lease of IT materiel or systems. Services will include training, education, consulting and on-site technical support.

Figure 1.

SSN Reduction Plan Phase 1 and 2 Results

By Steve Muck

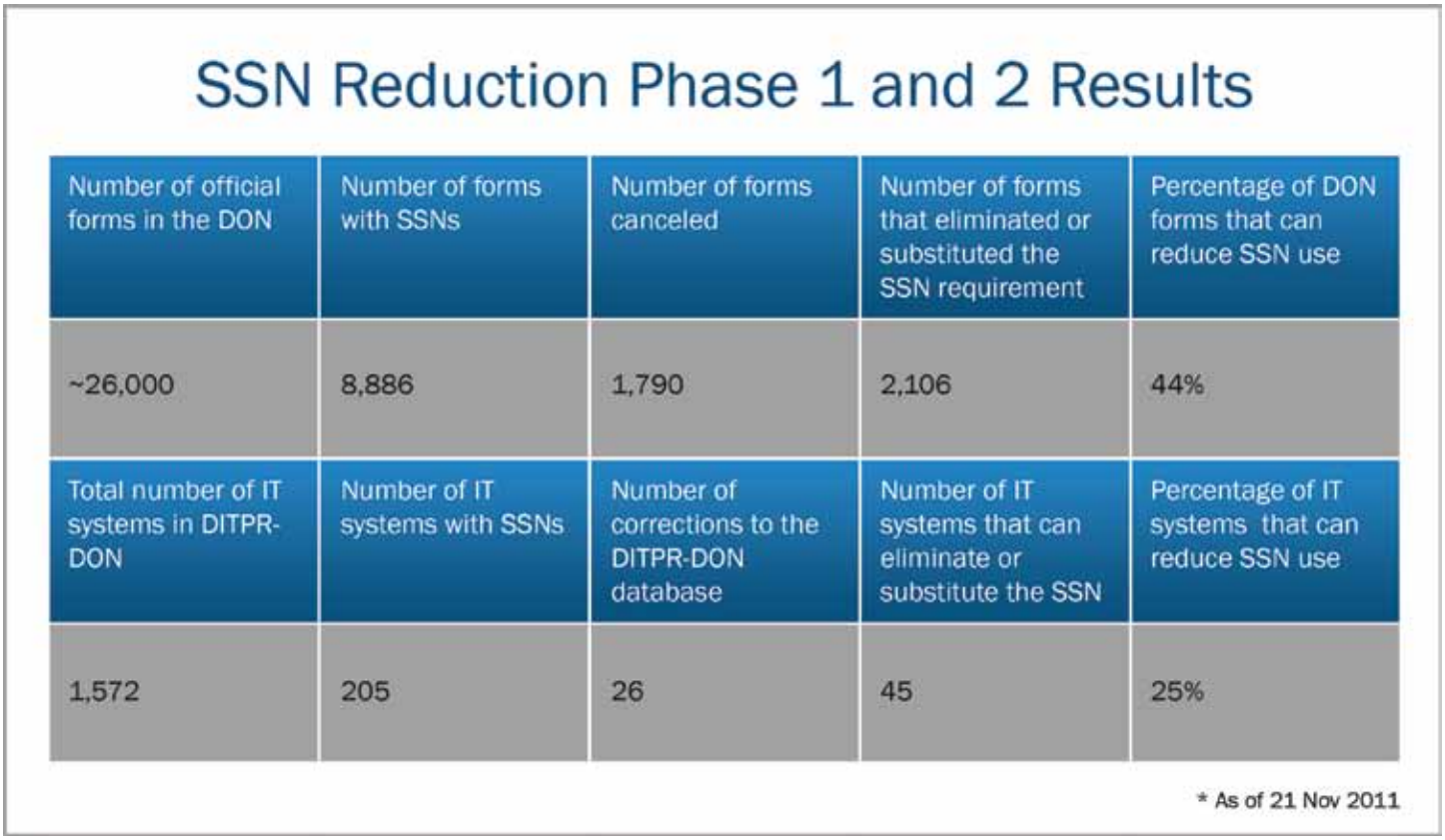
The Department of the Navy continues to implement guidance to better safeguard personally identifiable information (PII) by reducing or eliminating the collection, use, display and maintenance of a Social Security number (SSN) where possible. During the past 18 months, the DON has implemented two phases of its SSN reduction plan and is initiating procedures for the third phase. Results of this departmentwide effort are detailed below.

During Phase 1 of the SSN reduction plan, all official DON forms collecting SSNs were reviewed and justification was required for the continued collection of SSNs. This phase further required eliminating all unofficial forms that collect PII and posting all official forms to the Naval Forms Online data repository. After reviewing more than 26,000 forms, Navy and Marine Corps forms managers eliminated the collection of a SSN by 44 percent. Phase 2 required review and justification for continued SSN collection and use for all information technology systems registered in the Department of Defense IT Portfolio Repository (DITPR)-DON and Defense Health Program System Inventory Reporting Tool (DHP-SIRT). Navy and Marine Corps information technology system program managers and privacy officials identified 45 IT systems that can either eliminate or substitute a SSN with another unique identifier. To date, both reviews have resulted in significant reductions of SSN collection, use, display and maintenance.

By January 2012, Phase 3 of the SSN reduction plan will be implemented across the department. This next phase will provide the means to substitute the electronic data interchange personal identifier, now referred to as the DoD identification number, in place of a SSN where possible. Phase 3 will also place restrictions on using a SSN in memorandums, letters, spreadsheets, and hard copy and electronic lists. Faxing documents containing a SSN will also be restricted.

PII breach metrics suggest that SSN reduction efforts are working. Breaches involving SSNs have declined by 20 percent during the past 12 months. While these efforts have or will significantly reduce SSN use, there is still more work to be done. Owners of systems and forms citing interaction with other DoD or DON systems as a reason for continued use of SSNs must regularly review the requirement and reduce or eliminate SSN use when a change in the other system makes it possible. For a list of the approved use cases for systems collecting SSNs, please go to the DON CIO website: www.doncio.navy.mil/ContentView.aspx?id=1833. CHIPS

Steve Muck is the privacy lead for the Department of the Navy Chief Information Officer.



Safeguarding PII on Shared Drives Continues to be a Challenge

The following is a recently reported personally identifiable information (PII) data breach involving the posting of a large number of documents containing PII on an activity's shared drive. Incidents such as this will be reported in CHIPS magazine to increase PII awareness. Names have been changed or omitted, but details are factual and based on reports sent to the Department of the Navy Chief Information Officer Privacy Office.

Background

Shared drives facilitate information sharing and collaboration. Their availability and ease of use make them a popular tool across the DON. However, the number of PII breaches submitted related to shared drives has not decreased. Posting personal information in shared drive folders that do not have access controls, or where the access controls have been removed, continues to be an issue.

The Incident

In November 2011, during an activity's detachment swap prior to deployment, a backup file containing employment information, including names, Social Security numbers (SSN), resumes, hiring information, disability information, etc., was created because of network connectivity problems. The backup file was posted on the activity's shared drive, but was not encrypted. No password protection was established for the file — meaning that access was not restricted to only those with an official need to know.

Approximately a month after the backup file was posted to the shared drive, an employee discovered it, recognized that it contained personal information and reported it during a staff meeting. An investigation was immediately initiated and steps were taken to restrict access to only those with a need to know. A PII breach report was submitted to the DON CIO.

The investigation involved identifying individuals by name and the PII elements contained in the files associated with each of the affected personnel. Using this information, the DON CIO Privacy Office directed the activity to notify those individuals whose sensitive PII had potentially been compromised.

Lessons Learned

When posting personally identifiable information on a shared drive, positive controls that restrict access to only those with an official need to know must be in place. Positive controls include encrypting documents and password protecting files and folders containing the documents. Collecting only the PII elements necessary to perform the mission is also an important consideration.

It is important to note that maintenance performed on shared drives often involves the removal of access controls. Following maintenance, it is important to ensure that the controls have been properly restored and to verify they are working correctly.

Activities should perform routine spot checks and searches on their shared drives using key words such as "SSN," "Social Security number," "DOB," "date of birth," etc. Where documents can be removed, they should be deleted. Files and folders containing PII should be protected with the appropriate permissions. In some cases, PII can be redacted from documents and the resulting document saved. The collection of SSNs should be authorized by one of 12 approved use cases. The list can be found on the DON CIO website at www.doncio.navy.mil/ContentView.aspx?id=1833.

Documents in files and folders on shared drives should also be marked "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

The DON CIO website contains several privacy articles, tips and naval messages that address the protection of PII on shared drives. Visit www.doncio.navy.mil/privacy. CHIPS

Steve Muck is the privacy lead for the Department of the Navy Chief Information Officer.

NMCI continues to provide solutions for Sailors and Marines

Services include convertible laptops, a Hosted Virtual Desktop, Win 7

From the Naval Enterprise Networks Program Office

With all of the excitement surrounding the release of the Next Generation Enterprise Network (NGEN) Request for Proposal (RFP), the operation of the Navy Marine Corps Intranet (NMCI) continues to mature with the implementation of new solutions and security measures designed to help Sailors and Marines perform their mission critical tasks more effectively and efficiently.

The Naval Enterprise Networks (NEN) program office, which manages the NMCI and NGEN programs, is deploying a number of new Navy initiatives including tablet laptops for Navy recruiters, a Hosted Virtual Desktop (HVD) capability, expanded support for smartcards used to authenticate the identity of NMCI users, an enterprise-wide operating system upgrade and improved end user hardware delivery times.

All of these items pace with today's technology and support the Department of the Navy's (DON) efforts to develop mobile solutions to provide access to the right data at the right time and in the right place.

"The importance of the current network to the DON is not lost on the program office," said Capt. Shawn P. Hendricks, NEN program manager. "We are focused on continuously improving NMCI to make it more agile, flexible and useful to our users. NMCI is critical to the day-to-day operations of supporting our Sailors and Marines."

Mobile Recruiter Initiative

In early 2011, the Navy Recruiting Command (NRC) approached the NEN program office with a request for a highly capable tablet-style laptop with a sufficient "wow factor" to be on par, if not exceed, the devices used by the Army, Air Force and Marine Corps recruiters in the common quest to recruit today's tech-savvy youth. Attempting to impress potential candidates with years-old laptop technology proved to be ineffective — Navy recruiters needed state-of-the-art technology to help them convey the image that today's Navy knows how to effectively utilize modern information technology.

The new Navy recruiter laptops also had to be highly capable in hardware computing power with built-in Wi-Fi and 3G (third generation mobile telecommunications) broadband radios, a tablet form factor to support taking candidate applications in the field, strong security with full-disk encryption that is Department of Defense (DoD) Common Access Card (CAC) enabled, electronically configurable and maintainable via the Internet. The mobile recruiter laptop had to fully support the needs of the Navy recruiter corps.

Working with the NRC, the NEN program office agreed to equip recruiters with a convertible laptop, one in which the screen can swivel 180 degrees into position to function as a tablet device with touch screen capabilities while retaining the full computing power and functionality of a traditional laptop. Apple's iPad and other dedicated tablet devices were considered, but ultimately the recruiters decided that tablets do not deliver the computing power and security capabilities that they need.

For security and maintainability, the Mobile Recruiter solution includes the capability to remotely manage and update recruiter laptops in the field, wherever they are being used. Through an agent-based (i.e., software installed on the laptop), mobile network access control (NAC) capability, security policy updates, software configuration changes and even new applications are electronically "pushed" to laptops over the Internet, while transparent to users.

The Mobile Recruiter initiative has essentially expanded the reach of the NMCI enterprise to the Internet-based mobile platform.

Three potential devices were identified and field tested by the NRC. In the end, the NRC chose the Hewlett-Packard (HP) Elitebook 2740p Tablet PC because it met the wow factor criteria, as well as ease of use, ample computing power, long battery life and price point. The NRC's initial order was for more than 4,800 Elitebook laptops.

Since the task order was awarded in May 2011, HP, the prime contractor for the NMCI, finished developing the solution and achieved Interim Authority to

Mobile Recruiter Initiative Kit – a convertible laptop, printer, scanner and speaker.

Operate (IATO) in just three months. HP ramped up production at its Mechanicsburg, Pa., staging facility to more than 105 seats per day, and seat shipments to the Navy Recruiting Districts (NRD) commenced soon after.

The NRC began rolling out Elitebooks to recruiters in early September 2011. The feedback from recruiters has been positive; the tablet laptops are appealing to potential recruits and are effective in increasing the recruiters' productivity. The device has been so popular that NRDs not slated to receive seats until later in the deployment schedule have asked to receive their laptops earlier.

"High school students are impressed when they see the technology I am using and can't help but wonder what other futuristic technologies the Navy is using," Naval Aircrewman 2nd Class Mickey Blasingame reported to the Chief of Naval Personnel following a demonstration of the Mobile Recruiter Initiative Kit, a convertible laptop, printer, scanner and speaker.

"The capabilities of the Mobile Recruiter solution have allowed us to complete double the tasks in literally half the time, boosting production and improving morale by allowing recruiters to shorten the average workday, all while saving countless dollars in travel and man-hours," Blasingame said.

Hosted Virtual Desktop

In April, the NEN program office will begin a limited deployment of the Hosted Virtual Desktop solution, which is more commonly known as a thin client.

The HVD will use a new thin client device that is basically a keyboard, monitor and mouse with a CAC reader and Universal Serial Bus (USB) ports for local devices. The HVD connects to a server where all of its software and data are stored.

The difference between a regular workstation, also known as a thick client, and an HVD is the lack of a hard drive. It is replaced by a flash memory module, which contains a small, solid state drive.

Each user will have an HVD and up to 30 gigabytes (GB) of network storage, replacing the traditional, stand-alone computer hard drive.

The advantage of an HVD is improved security, accessibility to data files and operational efficiency while decreasing operational costs. Benefits include:

- Deploys security patches and software updates on the server level rather than the individual workstation level, thereby increasing the productivity of users.
- Simplifies the day-to-day management of calls to the NMCI service desk. Currently, if a user has a problem with the computer system or an application, a service desk technician takes control of the user's computer for remote repair. With the HVD, the issue can be fixed on the server level without affecting the user.
- Decreases the threat of a security breach because servers are equipped with more stringent security protocols than an individual workstation.

The key to making the HVD a viable replacement for a regular workstation is ensuring that the user experience — processing speed and access to storage, applications and the Internet — is equal to or better than a standard workstation.

Applications are one of the biggest challenges in implementing the HVD. Every application that an HVD user needs must be certified, virtualized and loaded on the server. Due to the certification and virtualization requirement, the HVD deployment will begin with unclassified desktop users who primarily rely on Microsoft Outlook and the Microsoft Office suite of applications.

Win 7 Deployment

The NMCI team completed a limited Navy deployment pilot (450 seats) of the Windows 7 operating system. Lessons learned from this pilot will benefit the enterprise deployment of Win 7. Applications and peripheral device drivers are being certified and the Navy's enterprise-wide deployment began in January 2012.

The transition to Win 7 begins the NEN program office's efforts to transition all NMCI seats from Windows XP to Win 7 prior to Microsoft's April 8, 2014, end of life cycle support date. All seats with Win XP must be removed from the network after that date.

The initial Win 7 deployment will be to Non-secure Internet Protocol Router (NIPR) desktops deployed via seat refresh or new seat delivery processes. Other assets, including NIPR laptops, Secure Internet Protocol Router (SIPR) seats, "Deployable" seats, etc., will be Win 7 certified following the NIPR deployment. Once all of the Win 7 solutions are available, user migration to Win 7 will become mandatory. An in-place upgrade is also under development to support those users on NMCI seats not eligible for technology refresh in the next two years.

With Win 7, users should expect enhanced NMCI user capabilities, such as faster file copying and the ability to multitask without affecting system performance through the new technologies, tools and software available on a Win 7 seat.

Increased Smartcard Support

The security side of NMCI has also improved via efforts to increase the use of smartcard credentials used for network authentication on both unclassified and classified NMCI seats. In August 2011, the NMCI team — working with Naval Network Warfare Command (NETWARCOM), Fleet Cyber Command (FLTCYBERCOM), the Navy Designated Approval Authority and the Naval History and Heritage Command (NHHC) — successfully demonstrated interoperability with Personal Identity Verification (PIV) smartcards issued by non-DoD agencies and departments. A Department of Homeland Security (DHS) user assigned to NHHC successfully utilized the DHS PIV smartcard to enable a NMCI account and access the NMCI network.

The ability to utilize a DHS or other federal agency PIV to access the NMCI increases productivity and efficiency since a separate CAC would not need to be issued to a user. Prior to the successful support of DoD-approved external identity credentials, it would have taken several days for the DHS user to be issued a DoD CAC. With FLTCYBERCOM and NETWARCOM now managing certificate trusts in NMCI, users issued non-DoD PIV credentials can access the NMCI and smartcard-enable their NMCI account as soon as their account is provisioned.

This accomplishment is also a significant milestone toward complying with Homeland Security Presidential Directive (HSPD) 12 and numerous DoD, DON and U.S. Navy policies that require the use of a standardized PIV identity credential to access government information systems.

On the classified side, the NMCI recently became the first DoD enterprise network to fully support the SIPRNET smartcard token for user authentication.

NMCI actively participated in a DoD initial operational test and evaluation (IOT&E) for a DoD-issued smartcard that will be issued to all SIPRNET users over the next two years. The smartcard will be used for authenticating user identity to SIPRNET networks and digitally signing and encrypting SIPRNET email, similar to how the CAC is used on the NIPRNET. The DoD IOT&E also involved members of the Program Executive Office Command, Control, Communications, Computers and Intelligence (C4I), Space and Naval Warfare Systems Command (SPAWAR) System Centers Pacific and Atlantic, NETWARCOM, FLTCYBERCOM and the Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6).

The new SIPRNET capability resulted in the NMCI SIPRNET deployment of smartcard middleware, 90Meter's Smartcard Manager, and a Web-based tool which enables a user's account for use with a SIPRNET smartcard.

By implementing two-factor authentication using a SIPRNET smartcard token, network security is increased since a user must present something they have (the SIPRNET token) and something they know, the SIPRNET token's personal identification number (PIN), prior to being granted access to the network. From a network user perspective, this capability also provides end users with an opportunity to contact the NMCI service desk and "enforce" their account for smartcard authentication, thereby eliminating the need to remember and frequently reset their SIPRNET account password.

The DoD Chief Information Officer released an Oct. 14, 2011 memo, "DoD SIPRNET Public Key Infrastructure Cryptographic Logon and Public Key Enablement of SIPRNET Applications and Web Servers," which describes the plan to mandate enforcement of SIPRNET token authentication in mid-2013.

Five-day Seat Deployment

In September 2011, the program office began testing a five-day seat deployment initiative to speed up the delivery time of new workstations to Navy commands that did not require an installation of infrastructure.

When the NMCI Continuity of Services Contract (CoSC) began in October 2010, it took an average of 64 business days for a new seat to be delivered under the new contract (versus 25 business days under the original NMCI contract that ended Sept. 30, 2010) because under the CoSC workstations were procured as commands ordered them and were no longer forward supplied in a warehouse.

Hendricks and his staff worked with prime contractor HP Enterprise Services to identify an acceptable accelerated delivery timeline resulting in a "five-day deployment" from the time a new seat is ordered.

Many challenges were overcome in developing the five-day deployment initiative, including the development creation of a new request and delivery process. To date, two pilots with a total of 63 seats have been completed, validating the feasibility and success of a five-day deployment.

The program office is still analyzing and tweaking the process, but the five-day seat deployment initiative is expected to be available enterprise-wide in early 2012.

The NMCI team remains dedicated to continuous improvements in security, reliability, agility and effectiveness through the implementation of emerging technologies. While NGEN has the attention of the DoD, DON and industry, NMCI continues to provide the mission critical network services that support the men and women of the U.S. Navy and U.S. Marine Corps. CHIPS

For more information contact the PEO EIS public affairs office at PEOEIS_PublicAffairs@navy.mil.

Convertible laptop – the screen can swivel 180 degrees into position to function as a tablet device with touch screen capabilities while retaining the full computing power and functionality of a traditional laptop.

NMCI By-the-Numbers

- More than 700,000 users;
- 384,000 workstations and laptops in more than 3,000 locations from major bases to recruiting offices;
- More than 3.4 terabytes of data transported and 124 million browser transactions made per day;
- More than 2 million unauthorized access attempts blocked annually;
- An average of 60 new viruses detected and removed from NMCI each month;
- More than 4,000 potentially hazardous email attachments stripped each day;
- Three enterprise service desks provide 24-hour a day assistance via email and telephone;
- 38 classified and unclassified server farms, 28 micro-server farms; and
- Four network operating centers provide redundancy and fail-safe security for network information.

Follow NMCI and PEO EIS on Twitter:
@PEOEIS
@NMCIEnterprise

Negotiating Contracts for Cloud-Based Software

Any cloud service level agreement should contain specific, measurable and enforceable terms and conditions

By Gretchen Kwashnik

The federal government's "cloud first" policy, as part of the Federal Chief Information Officer's "25 Point Implementation Plan to Reform Federal Information Technology Management," requires federal agencies to consider cloud computing before making new IT investments and to move at least three applications to the cloud by May 2012.

Requests for information, issued by the Department of the Navy in July 2011, indicated that the Next Generation Enterprise Network (NGEN) will transition to a cloud-based delivery model. In an August 2011 media roundtable, the Department of the Navy CIO, Mr. Terry Halvorsen, said cloud computing, along with thin-client and zero-client technologies, are some of the models that the DON can use to cut 25 percent from its business IT budget in the Future Years Defense Program financial plan.

With the department's goals to decrease IT costs, improve deployment speed and agility and operate more efficiently will come shifts in IT funding. For example, there are funding allocation differences between the traditional procurement of IT licenses, which are normally capital expenses that are depreciated over time, while the subscription procurement model for cloud services is normally an operational expense that is not depreciable.

The cloud concept encompasses a variety of service models: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS). These service models can be delivered in a variety of ways, from a private cloud (operated solely for an organization whether hosted internally or by a third party over a virtual private network), a public cloud (operated by a third party over the Internet), or a hybrid cloud that combines private and public clouds to coordinate a solution.

In all instances, the difference from traditional procurement is that some or all IT resources (hardware, software and support services) are rented instead of purchased as perpetual software licenses, thus creating the hardware infrastructure to support software and data, and maintaining the selected solution.

SaaS, which is the most widely adopted service delivery model in these still-early stages of cloud computing, provides a timely example of negotiating "cloud first" contracts. From an overall contractual perspective, the SaaS cloud model does not vary greatly from traditional on-premise software licensing because the same quality of software and functionality is supplied by a software provider. However, a few of the key licensing differences are in the granting of a software license and payment terms.

Grant Software Licenses

With the cloud delivery model, software use is subscription-based and paid on a monthly or annual basis. In contrast, traditional software is normally purchased for perpetual use with one lump sum payment upfront. It is important to understand that sometimes traditional on-premise software can also be offered via a subscription model.

Perpetual Licensing: When purchasing the right to use a software license in perpetuity, the full license rights may depend on how payment terms are structured. Perpetual licensing is not an option for SaaS through a public cloud. Whether this perpetual licensing model will be available for private or hybrid clouds is yet to be seen; it may depend on the ability to move existing applications into a private cloud. However, there are software providers that are making it easier to set up such private cloud instances.

Subscription Licensing: This is the most common licensing model for public cloud solutions, and it allows use of the software service only while the subscription is current and valid. Subscription licensing may be possible for hybrid cloud solutions where terms can be negotiated in the following ways:

– Paying a maximum subscription licensing fee over a specific term of service. Thereafter, the subscriber would have the right to use the software in perpetuity or exercise the option to use it in perpetuity for an incremental pre-negotiated fee. When using this type of subscription payment plan, users must ensure that the correct type of appropriation is used for the investment.

– Separating the hosting fees from the software licensing fees so the two are not intermingled.

Payment Terms

With traditional software licensing, you may be able to negotiate withholding a portion of the licensing fees until after the go-live or acceptance date of the software. Maintenance fees also may not be required until after the go-live date. Alternatively, cloud solutions bundle together hosting, software licensing and maintenance into one monthly or annual fee. Subscribers begin paying for the service as soon as they authorize the cloud provider to turn it on, even though the subscribers may not be using it yet.

To mitigate the financial risks in this practice, determine if the provider has a sandbox or proof-of-concept environment in which potential subscribers can become familiar with the software at little or no charge before signing a contract for a specific term and number of users. Any payment and financing terms must be in accordance with Federal Acquisition Regulation (FAR) Subpart 32.2, Commercial Item Purchase Financing.

SaaS Service Level Agreements

When using a SaaS provider, the focus is no longer on managing the technical software application, but rather the vendor relationship. This is where IT contract negotiation, contract management and supplier management skills come into play. All rights and responsibilities associated with the relationship should be included in an enforceable contract and effectively managed. The specific risks to be addressed in the contract with a provider will depend on the application, its business criticality, and the data that will be exchanged, stored and maintained by the provider.

CHARLESTON, S.C. (Oct. 7, 2011) Senior U.S. Navy officials tour the new data center at SPAWAR Systems Center Atlantic. U.S. Navy photo. SPAWAR is playing a pivotal role in the DON s data center consolida tion plan, as well as other IT efficiency and operational effectiveness efforts, to reduce IT costs and gain greater economies of scale.

Any cloud service level agreement (SLA) should contain specific, measurable and enforceable terms and conditions. If the SaaS provider fails to meet an obligation under the SLA, the agreement must have the "teeth" to mitigate a failure from happening again. For example, the SLA should contain specific remedies that apply when obligations are not met, including financial penalties or credits for future services. The best remedy may be a refund since the value of a credit against future services from a provider that has already failed does not guarantee reliable service.

A Word about Security

Any selected cloud solution must conform to federal security requirements, including Federal Information Processing Standard (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," and the Federal Information Security Management Act (FISMA), and have an Authority to Operate (ATO) through the Federal CIO Council's Federal Risk and Authorization Management Program (FedRAMP). Cloud solutions can be validated for multi-agency use, which supports the standardized approach to cloud computing across the DoD advocated by the DoD CIO. A list of solutions already approved through FedRAMP can be found at www.gsa.gov. Solutions without an ATO will require working with the vendor through the FedRAMP program.

With federal initiatives like cloud first, green IT and continuous (security) monitoring, cloud solutions will play an increasingly greater role in DON and DoD IT strategies. To be successful, IT stakeholders must better understand how to procure and implement cloud-based offerings. CHIPS

Gretchen Kwashnik provides contract support to the DoD Enterprise Software Initiative (ESI) and DON CIO.

Rear Adm. Grace Hopper and the *Nanosecond*

Anyone who met Grace Hopper probably heard her talk about the "nanosecond." Hopper liked to use visual examples when she spoke, and she frequently advised young naval officers and programmers not to waste time — not even a nanosecond. She used a foot-long strip of wire to represent a nanosecond, which is equal to the distance traveled by an electron along the wire in the space of a nanosecond — one billionth of a second. She sometimes contrasted the example with a microsecond by flourishing a coil of wire nearly 1,000 feet long that the wiry admiral could easily manage with a steady wrist.

Hopper left a lasting impression of immense energy and razor sharp wit, quickly disproving any notions of a frail, white-haired woman. While serving in the Navy from the late 1960s until her retirement in 1986, Hopper's legendary energy was focused on desktop technology deployment Navywide.

Hopper was a familiar face at Navy Micro conferences and was frequently followed by an entourage of admirers. She could be intimidating because she always challenged the status quo.

Through the years as CHIPS editor, I have met many naval officers and civilians who remember her fondly. They comment on her remarkable vision for the future. The nanosecond is always a favorite story and so is her tagline, "Remember, it's always easier to ask forgiveness than it is to get permission." CHIPS

Sharon Anderson

The First "Computer Bug"

A moth found trapped between points at Relay #70, Panel F, of the Mark II Aiken Relay Calculator while it was being tested at Harvard University, Sept. 9, 1947. The operators affixed the moth to the computer log, with the entry: "First actual case of bug being found." They put out the word that they had "debugged" the machine, thus introducing the term "debugging a computer program." In 1988, the log, with the moth still taped by the entry, was found in the Naval Surface Warfare Center Computer Museum at Dahlgren, Va.

Courtesy of the Naval Surface Warfare Center Dahlgren Division, Naval History and Heritage Command Collection.

Protecting Information in a Cloud Computing Environment

A checklist for practitioners

The need to protect the confidentiality, integrity and availability of information hasn't really changed much in the last 100 years

By Brian Burns

The problems with data security can be solved by learning from the past and using the technology of the future. We have transformed from the industrial age to the information age and now are moving to the collaboration age. As nanotechnology and robotics evolve, we will transform to the embedded, or immersion age, where we will work and live in virtual reality side-by-side with robots and embedded nanotechnology devices. But for now, cloud computing services are the next step along the information management journey.

Back to Basics — Information

The National Institute of Standards and Technology's (NIST) Special Publication 800-145 defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing facilitates the use of information. The warfighter and business professional need information to make informed decisions. Hence, information confidentiality, integrity and availability (CI&A) must be protected. The definitions for information, information systems and national security systems are defined in OMB Circular A-130, 44 United States Code (USC) 3502(7), 40 USC 11103(a)(1) and 44 USC 3542(A).

The Office of Management and Budget (OMB) Circular A-130 defines information as "any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms."

44 USC 3502(7) defines an information system as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information." OMB Circular A-130 adds to the end of this definition: "in accordance with defined procedures, whether automated or manual." So would you like your information in paper, plastic, plasma, metal, mineral, crystal or wave form?

Information 100 Years Ago

Assume a person had information in the form of a drawing, photograph or text on paper. The type of information would dictate the form, such as a time and date stamp on time-sensitive data or a raised seal on an official document. If the information was confidential, it was probably sealed in an envelope and stamped with an imprint or wax seal. The value of the information would decide how someone handled it. Information of no value was probably thrown away.

If of low value, the document might have been left on a person's desk. If of moderate value, it was probably placed in a folder, tagged with a reference code and stored in a file cabinet.

A document of high value was probably locked in a fire-proof cabinet, and if of national security value, additional controls most likely included storage inside a vault with guards and restricted access.

In the previous cases, access to the data was necessary. If the confidentiality, integrity or availability was compromised, the custodian of the information was at risk for breach of service, security or privacy violations, possible monetary damages, and civil or criminal charges. The owner of the data was responsible for ensuring its CI&A to those with the authority to access the information. Law enforcement authorities were responsible for prosecuting the custodian and the entity that caused the confidentiality, integrity or availability breach in cases with civil or criminal penalties.

The tenets for information CI&A security are the same in cloud computing. Assume a person has a geospatial map, an image, or electronically formatted or unformatted text. If the information is an official document, digital signatures can be used. If the information is confidential, it may also be encrypted and stored in a restricted database repository.

Meta tagging information can provide context to the information in a geospatial map, an image or electronic text. Meta data can include information regarding when and who created, modified and stored the data. Several standards have emerged for tagging data, such as C2 Core for command and control information. Tags could include fundamental information, such as the content, context, authoritative source, location, duration/expiration, and the security and privacy classification level. Cloud computing has not changed the way we handle information based on value and classification levels. If the information has no value, such as a non-federal record or a document not under a litigation hold, it could be thrown away, though the trash can may be on a computer desktop.

Low-valued information can be stored nearly anywhere (shared public or private cloud) with minimal controls. As long as there is a backup copy, the integrity of the information can be easily restored if it is compromised. If the information is of moderate value, it could be encapsulated and stored in an electronic folder, tagged with a reference code and stored in an electronic file directory or database repository. The information may be located in a shared public or private cloud.

The most valuable information would be encrypted and stored in a restricted electronic file directory or database repository, most likely in a private cloud. If of national security interest, the information would be tagged, encrypted and stored on a secured server in a restricted data center facility in a private cloud. Authorized availability of the information is necessary, and the guardians of the information are held accountable for its security, with consequences of financial penalties, or civil or criminal charges

if they fail, within the appropriate law enforcement and contract governance jurisdiction.

Information Security

The confidentiality, integrity and availability of data will be potentially bound by the intersection of user authentication <with> user authorizations <with> device authentication <with> data tagged attributes <with> device location <with> information encryption. A summary of personal identification policy is shown in Figure 1.

The Air Force is currently defining authoritative data sources, tagging data, consolidating data centers and assessing the information and security classification levels that would require a private, public or hybrid cloud; defining identity and access management (IdAM) and governance; and as part of Air Force IT efficiencies, assessing Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) models.

The fundamental information security and privacy concerns in cloud computing are:

If the CI&A of the information is compromised, does the government have jurisdictional authority to prosecute the involved parties? This security concern is more of a contract governance concern than a technical one.

Does the government have the authority and ability to continuously monitor and audit the service providers' operational and technical controls?

Can cloud computing service providers meet the performance measures and demonstrate adequate protection, mitigation, recovery and discovery for the information?

A risk assessment of cloud computing security and privacy must be considered to ensure a secure solution is operationally viable to support government data. NIST Special Publication 500-291, "Cloud Computing Standards Roadmap," and the Federal Risk and Authorization Management Program (FedRAMP) provide a standard approach to assessing and authorizing (A&A) cloud computing services and products. Consulting federal cloud computing experts, such as Earl Crane of the Department of Homeland Security (DHS), will help to identify a number of security controls and evaluation criteria. When considering available federal resources and advanced persistent threats, some security considerations, controls and guidelines will be of greater importance than others, including the following.

A Methodical Approach

Establish an information-centric risk assessment and authorization baseline for using cloud computing shared resources in line with government standards, policy and guidelines.

Transition from the traditional system development life cycle to an information management life cycle where the focus shifts from system ownership and design to information confidentiality, integrity, availability and authorized use through service offerings.

Apply the appropriate integrity controls for service models. For example, SaaS environments focus on application integrity, such as input validation, while IaaS environments focus on file system and database integrity.

Develop cloud portability and interoperability standards to improve government information sharing between systems and the public; and reduce application and storage reengineering and interoperability costs.

Evaluate cloud compliance with system and communications protection requirements by considering compartmentalization, isolation, external and internal connections for system boundaries, routing through government authorized trusted Internet connections for perimeter protection, and domain integrity requirements, such as Domain Name System Security Extensions (DNSSEC).

Address policy and procedure cloud computing paradigm service changes to traditional government system boundary definitions, compartmentalization and inventory identification associated with data center operations and maintenance, configuration management, and physical and personnel security. The dimensions of cloud computing are shown in Figure 2.

Technical Considerations

Shift encryption and media protection from system-centric to an information-centric approach in a cloud computing environment. Data may need to be encrypted when stored and transmitted through the infrastructure to its authorized user destination. Digital rights management may be required to protect the confidentiality, integrity and information owner's intellectual rights.

Coordinate encryption key management with identity, credentialing and access management to maintain control over information stored within a cloud and distributed through multiple access paths. Maintaining the physical and logical separation of the information storage from encryption key management may be required to protect the information confidentiality and integrity. Otherwise, unauthorized entities may gain the "keys to the kingdom" to the information.

Monitoring

Require application security controls, including code reviews, vulnerability assessments and independent validation.

Identify if government-specific security and performance requirements may not be obtainable through commercial cloud computing services. These may include personnel security background checks, which are mandated controls (and not at the discretion of the contracting government agency), operational standards, management practices and technologies.

Require additional visibility into the cloud computing service providers' infra-

Personal Identity Verification Policy

- Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors.
- OMB Memorandum M-04-04: E-Authentication Guidance for Federal Agencies.
- FIPS Publication 201-1: Personal Identity Verification of Federal Employees and Contractors.
- NIST SP 800-63: Electronic Authentication Guideline.
- NIST Special Publication 800-73-3: Interfaces for Personal Identity Verification (4 Parts).
- NIST SP 800-76-1: Biometric Data Specification for Personal Identity Verification.
- NIST SP 800-78-3: Cryptographic Algorithms and Key Sizes for Personal Identity Verification.
- Personal Identity Verification Interoperability For Non-Federal Issuers issued by the Federal CIO Council May 2009.

Figure 1.

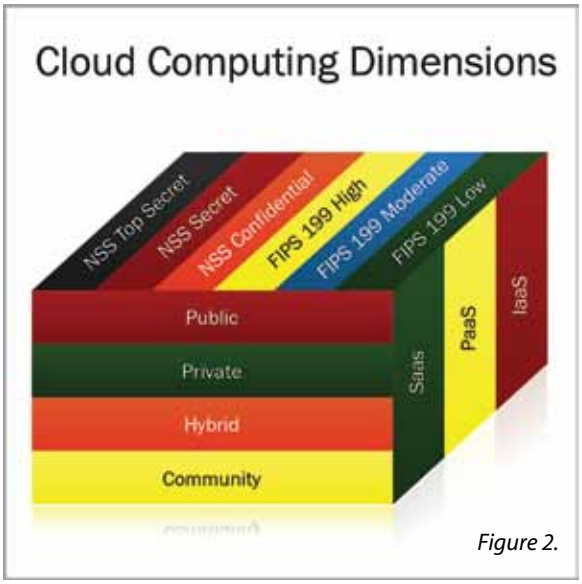


Figure 2.

Analyze the cloud service providers' contingency plans and service level agreements to ensure they meet government requirements and conduct periodic reviews to address changes in requirements.

structure environment to perform audits and to implement robust evaluation criteria in compliance with government laws, regulations and policy. This is driven by the requirement that the respective government system and data owner authorizing official's accountability cannot be outsourced.

Require the service provider to perform continuous monitoring and near real-time audit capabilities and technologies that apply accepted general audit principles.

Apply specific tools and techniques to the deployed technology, architecture and cloud service models to provide visibility of virtualization and resource abstraction for security operators within a virtualized environment.

Compliance

Require the cloud computing service provider to implement government security, privacy and performance incident response guidelines and requirements and to accurately assess and capture appropriate evidence.

The response plans should address the possibility that incidents, including privacy breaches and classified spills, may affect cloud services and other cloud customers. This requires identification of the specific tools, techniques and training that cloud computing service providers are required to provide for complying with government security and privacy incident responses, computer forensics and evidence for the chain of custody in a cloud.

Identify and control the physical location of data and access to the cloud environment for privacy and confidentiality compliance, audit and redress requirements and breach notification issues. Review contracts, terms of service and cloud provider privacy policies to ensure compliance. Conduct privacy impact assessments and implement federal privacy requirements, such as the Fair Information Practice Principles and System of Records Notices, which are guidelines for collecting, storing and retrieving information in an electronic framework.

Analyze the cloud service providers' contingency plans and service level agreements to ensure they meet government requirements and conduct periodic reviews to address changes in requirements.

Identify the risk of cloud computing shared or pooled resources on governance, priority of services and performance during high volume or restricted volume periods of shared resource use.

Implement a cloud computing awareness and training program that focuses on the risks of information disclosure and data protection in concert with the Committee on National Security Systems (CNSS) Instruction No. 1253: "Security Categorization and Control for National Security Systems" and FIPS Publication 199: "Standards for Security Categorization of Federal Information and Information Systems" guidance.

The Future of Cloud Computing

Government agencies will move from data center consolidation to the cloud over the next few years. The intersection of identity management, credentialing, access management and data attributes will drive privilege management security solutions down from the network, system and document level to the data element level and expand the use of cloud computing. Over the next few decades, as IPv6 replaces IPv4 and robotics and nanotechnology emerge as mainstream solutions, data in the cloud will extend to new robotic devices that could interact with or be attached to humans. Continuous data feeds from unmanned land, sea, air and space vehicles will be commonplace in the cloud. Hence, the line between back office data centers and edge devices will blur into meshed node components capable of access to information from anywhere at any time. Will we have to rethink data center consolidation and cloud computing in terms of data center mobilization and cloud computing data forecasts?

Robots could provide their own mobile storage and computing power rivaling some of today's data centers. Intrusion prevention and network appliances could be replaced with interactive nanotechnology security and communication devices that attack and extinguish intrusions and viruses from within the internal operations of the robot, thus becoming the robot's autoimmune system. We will have to protect the exoskeleton exterior perimeter of the robot from physical, chemical and electronic threats, as well as the internal operations and health of the robotic system and information.

As robots interact in physical and virtual environments with humans and other transmission devices, will we have to adopt additional information and system infiltration virus protection models analogous to physiological immunology, environmental safety and viral and communicable disease control and prevention? The analogies of today's interactive environments will provide the cloud computing solutions for tomorrow. CHIPS

Brian P. Burns is a member of the senior executive service and the deputy director for warfighter systems integration in the Office of Information Dominance and Chief Information Officer, U.S. Department of the Air Force.

Ensuring Spectrum-Dependent Systems are "Up to Code" Saving Time, Money

By Thomas Kidd and Mark Rossow

To achieve the most efficient use of communications-electronics (C-E) resources, the required capabilities of systems and equipment should be met during the procurement phase — rather than investing in equipment that may require redesign or retrofitting after development. Therefore, it is more critical than ever in these budget constrained times that program offices and procuring officials take advantage of processes that ensure systems and equipment provide their intended capabilities with minimal rework.

The use of electromagnetic spectrum, or radio frequencies, is a common wireless enabler for many, if not most, new C-E systems. The proliferation of wireless spectrum use within the Department of the Navy continues to increase. As a result, access to electromagnetic spectrum for all wireless systems is no longer ensured.

The electromagnetic spectrum is a scarce and highly regulated resource used around the world. Ensuring spectrum support for DON systems is a critical and necessary requirement that must be initiated during procurement and in the earliest stages of system development. Systems must be designed to operate in the proper spectrum, or they may interfere with other systems or violate international treaties and regulations. Retrofitting systems to bring them into compliance with regulations is often much more expensive than properly designing them from the beginning.

Spectrum supportability — meaning the availability of radio frequencies for a given system in its intended operating environment — must be ensured for C-E equipment that use radio frequencies. The term also describes whether a system's spectrum use is in compliance with local regulations and international treaties. While the term is regularly used within the Department of Defense's spectrum community, it is critical that it is understood throughout the DON's operational and acquisition communities, which procure and develop spectrum-dependent systems and equipment.

Spectrum supportability entails a number of factors that include the location in which the equipment will be operating and its compatibility with other equipment, as well as safety factors. The process to ensure a high degree of spectrum supportability begins early in the acquisition process. Organizations must complete and submit a spectrum supportability risk assessment and an application for equipment frequency allocation. This ensures compliance with international, federal, DoD and DON spectrum policy.

The information provided in the assessment and application is used by personnel within the federal government, depart-

PACIFIC OCEAN (June 8, 2011) Aviation Electronics Technician 3rd Class Christopher Jiles, from Lemoore, Calif., reads schematics before troubleshooting the weapons systems on an F/A 18F Super Hornet from the Black Aces of Strike Fighter Squadron (VFA) 41 in the hangar bay aboard the aircraft carrier USS John C. Stennis (CVN 74). John C. Stennis is participating in a joint task force exercise off the coast of Southern California. U.S. Navy Photo by Mass Communication Specialist 3rd Class Timothy Aguirre.

ments of Defense and Navy, and host nations (nations that allow the United States access to their spectrum) to provide guidance for the successful acquisition of spectrum-dependent equipment and to ensure radio frequencies can be made available within the equipment's intended operational area. The completion and data requirements of the assessment and application are detailed in DoD Instruction 4650.01: "Policy and Procedures for Management and Use of the Electromagnetic Spectrum."

These documents are similar to building permits. While building permits assess zoning, water, sewage and other factors that encompass building construction, the spectrum supportability documents are reviewed to determine potential effects on the electromagnetic environment, as well as compliance with applicable regulations, treaties and guidance. These evaluations are intended to ensure that radio frequencies can be acquired in the equipment's intended operational area and that the use of the equipment will not degrade the effectiveness of other spectrum-dependent equipment in the same environment.

Additionally, consideration must be given to a system's electromagnetic environmental effects (E3). E3 considerations include radio frequency interference and potential detrimental effects from its use on other electronics systems (RF dependent or not). Electromagnetic environmental effects can degrade the performance and operational capabilities of guidance systems, weapons systems and munitions. In some cases, environmental effects have the potential to cause catastrophic events.

An equally critical aspect of spectrum supportability is the DON's requirement to be fiscally prudent with acquisition funds. The development or acquisition of spectrum-dependent systems that are not supportable wastes precious resources.

It is more than fiscally wasteful; it can result in the loss of necessary, and sometimes vital capabilities for the operational forces, which can heighten the risk of mission failure and injury. The need for efficient and effective use of funds cannot be overstated. The Office of Management and Budget requires agencies to ensure radio frequencies can be made available before estimates are submitted for the development or procurement of spectrum-dependent systems.

Just like building permits are updated to allow modifications, so too must spectrum supportability documents be regularly updated to remain current with acquisition and development changes. Updating spectrum data enables spectrum professionals to continually provide refined guidance to further ensure a system's spectrum supportability.

Completing and updating spectrum supportability documents provide acquisition professionals a level of assurance that the required radio frequencies will be available for the operation of the equipment. This, in turn, provides a similar level of assurance that funds will be spent on capabilities that can be employed by Sailors and Marines and will not be wasted on rework. CHIPS

NORFOLK (Sept. 9, 2011) The Virginia class attack submarine Pre Commissioning Unit (PCU) California (SSN 781) gets underway from Naval Station Norfolk to conduct weapons systems acceptance trials. California is the eighth Virginia class submarine and is scheduled to be commissioned Oct. 29. U.S. Navy photo by Mass Communication Specialist 2nd Class Danna M. Morris.

Thomas Kidd is the director for strategic spectrum policy for the Department of the Navy. Contact Mr. Kidd at DONSpectrumTeam@navy.mil. Mark Rossow provides strategic spectrum policy support for the DON spectrum team.

GOING MOBILE

New DON Mobile Contracts and Tools Drive Savings

By Mike Hernon

In today's efforts to identify and leverage all potential efficiency opportunities, one area often overlooked is a device that hundreds of thousands of Department of Defense personnel carry every day — their mobile phone. With voice and data plans sometimes costing more than $100 a month, the DoD spends tens of millions of dollars on cellular bills every month to ensure that personnel away from the office have access to the information they need to do their job. Such a large sum presents an attractive target for cost-cutting.

Cutting mobile costs does not mean organizations must diminish mobility capabilities. They do, however, need to optimize the environment ensuring that users are given the right mobile solution, at the right price, and with the ability to monitor use on an ongoing basis. In practice, this requires that commands have access to contracts providing favorable rates, telecommunications expense management (TEM) tools that provide insight into use and billing, and the ability to make changes easily and quickly.

All these capabilities are available to commands in the Department of the Navy (DON) through the enterprise contracts negotiated and managed by Naval Supply Systems Command Fleet Logistics Center San Diego (NAVSUP FLC San Diego, formerly known as Fleet Industrial Supply Center San Diego). Existing DON policy already mandates that all CONUS commands use these contracts, and a new DON policy in development will also require use of the TEM tools.

Leveraging the Contracts

The new enterprise cellular contracts drive costs down even more than the previous contracts, which have been very successful in controlling DON mobility spending during the past several years. The new contracts allow commands to compare prices for their business needs simultaneously across all four major providers. This maximizes competition and will allow the DON to see reduced pricing throughout the life of the contract. There are other cost-savings benefits to the new contracts in addition to lower plan pricing.

Other benefits include the ability to get free devices on any plan and unlimited texting, as well as tethering options, which provide laptop Internet connectivity without air cards that will result in substantial savings.

Early results prove the point as Rob Baker, command information officer (N6) for Commander, Navy Installations Command (CNIC), put it, "This new contract helps CNIC meet our part of the DON IT efficiency goals for cell phones and BlackBerrys because it reduces our spend[ing] by about $800,000 this year without reducing our critical mobility capability."

Cellular communications are a key component for the CNIC mission, and the ability to maintain the coverage the command requires at a reduced cost is a significant enabler of its effectiveness — as well as an efficiency effort.

Leveraging the Telecommunications Expense Management Tools

Getting the best prices for cellular services from the contracts is important, as seen from CNIC's experience. But commands also require the ability to effectively manage their cellular use and spending on a monthly basis to ensure that their mobile capability is truly optimized and cost efficient. These management controls are also available under the enterprise contracts via the Web-based TEM portals developed by each cellular provider. The portals have been designed specifically for the DON's requirements and contract specifications.

Through the portals, commands have access to electronic invoices and monthly usage and spending data. This data can be presented in myriad ways, including standardized and user-defined reports. Devices and service plans can be managed and changed online for immediate effect — either for entire commands or for just one user as appropriate. Monthly data can also be combined to conduct trend analyses over time.

To drive the maximum cost savings, TEM tools enable commands to easily identify some of the most common sources of wasteful cellular spending:

Zero-Use Lines. These are devices that accumulate monthly charges but are not used. They may be kept in reserve for continuity of operations (COOP) or they may be assigned to somebody who does not need a mobile device. By examining the data, the command can decide whether the device should be on a flat rate, in the case of a COOP device, or be canceled.

Excessive Overages. Most people try to avoid overages due to the high per-minute cost of services when the pool plan's limit is exceeded. However, in reality, a small number of overages to cover unforeseen circumstances is acceptable and can be cheaper than upgrading to a higher pool. Consistent overages of 125 percent or more, however, are considered excessive. These can now be easily identified, and the users can be placed on the proper plan.

Significant Underuse. In their zeal to avoid overage charges, some people may buy many more minutes than they will ever use — sometimes up to double the amount. This is as wasteful as paying for excessive overages. Paying for double the number of minutes actually used means paying twice what is necessary for the same level of service. Previously, underutilization was

BAIE DE GRAND GOAVE, Haiti (Jan. 27, 2010) A Sailor snaps a photo on his cell phone from the hangar bay of the multi purpose amphibious assault ship USS Bataan (LHD 5) of a vertical replenishment as an MH 60S Sea Hawk helicopter assigned to the Sea Knights of Helicopter Sea Combat Squadron (HSC) 22 picks up a load of humanitarian supplies from the Military Sealift Command fleet replenishment oiler USNS Big Horn (T AO 198). Bataan and the amphibious dock landing ships USS Fort McHenry (LSD 43), USS Gunston Hall (LSD 44) and USS Carter Hall (LSD 50) are participating in Operation Unified Response as the Bataan Amphibious Relief Mission by providing military support capabilities to civil authorities to help stabilize and improve the situation in Haiti in the wake of the 7.0 magnitude earthquake that hit the area Jan. 12, 2010. U.S. Navy photo by Mass Communication Specialist 2nd Class Kristopher Wilson.

difficult to identify, but today, TEM tools easily ferret out such information.

User Behavior. Some unnecessary costs may be avoided by modifying user behavior. TEM tools identify the practices and users that merit the most attention. One wasteful practice is the use of directory assistance. Cellular providers charge nearly $2 per call for this service. In many cases, the user could have easily looked up the number using the device's Web browser. Another costly usage charge is international roaming. Users planning international trips should have the proper international plan activated for their device prior to embarkation, otherwise significant roaming charges will apply. Charges can total thousands of dollars for one device for one trip. Once again, TEM portals permit this change to be made simply and online.

A Case Study in Efficiency

Through this multi-pronged framework of contracts, policy and automated TEM tools, Navy and Marine Corps commands across the enterprise are now positioned to optimize their cellular environment and realize significant cost savings — without impairing their mobility capabilities. CNIC's experience has shown the benefits of the strategic sourcing model that the DON has implemented for cellular services, which will continue to reap financial benefits for years to come. CHIPS

Additional information, the contracts, ordering guide and templates are available on the NAVSUP FLC San Diego website at https://www.navsup.navy.mil/navsup/ourteam/navsupgls/prod_serv/contracting/market_mgt. For DON telecommunications policy, visit the DON CIO website: www.doncio.navy.mil/telecommunications.

Mike Hernon is the former chief information officer for the city of Boston. He supports the DON CIO in telecommunications and wireless strategy and policy. You may contact the FLC San Diego team via cellmac@navy.mil.

Exercise Saxon Warrior 2011

U.S. and U.K. fine-tune link communications

By Lt. Dennis "Rickshaw" Szpara

Designed to build combat capability and foster cooperation between multinational forces and government agencies, Saxon Warrior 11, an exercise led by the United Kingdom's Flag Officer Sea Training (FOST) organization, was conducted off the southwestern coast of England in May 2011.

Several phases made up the eight-day exercise. The initial phase consisted of primarily single-mission scenarios, including surface, submarine and air combat, and several maritime security operations, such as counterpiracy, and visit, board, search and seizure. The exercise concluded in a full-scale "Thursday War" on May 26.

Although U.S. and U.K. forces responded to fictional geo-political and military scenarios, Saxon Warrior gave the "Bear Aces" of Carrier Airborne Early Warning Squadron 124 (VAW-124) the chance to carry out sustained and coordinated military operations with NATO partners. As part of the exercise, multinational aircraft squadrons practiced in low-level flight operations, air-to-air engagements, long-range strikes and close air support of surface combatants.

Other U.S. forces included Carrier Strike Group Two (CSG-2), Carrier Air Wing Eight (CVW-8) and Destroyer Squadron 22 (CDS-22), while United Kingdom participation involved various elements of the Royal Air Force and Navy.

To facilitate the integration of U.S. forces into the existing U.K. link architecture, the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific's network design team and the Joint Data Link Management Organization (JDLMO) created a Joint Tactical Information Distribution System (JTIDS) network library (JNL) for Link 16 to allow a common communication structure between all surface, air and land assets. With Link 16, military aircraft, ships and ground forces can exchange their tactical picture in near-real time. Link 16 also supports the exchange of text messages, imagery data and digital voice communications.

GULF OF OMAN (March 14, 2009) An E 2C Hawkeye assigned to the "Bear Aces" of Carrier Airborne Early Warning Squadron (VAW) 124 prepares to land aboard the aircraft carrier USS Theodore Roosevelt (CVN 71). Theodore Roosevelt and Carrier Air Wing (CVW) 8 are operating in the U.S. 5th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Andrew Skipworth.

Link Architecture for an Airborne Early Warning Squadron

JTIDS was developed to improve previous datalinks, bringing increased bandwidth, combat redundancy and greater geographic coverage. Through the use of a frequency agile receiver-transmitter and time sharing, large numbers of individual units can participate, monitor or relay tracks with no time delay. The key to this versatility lies in the software algorithms, which assign transmit and receive times, as well as the ability to select the data to be transmitted during these periods.

There are several versions of JTIDS software, each tailored to various mission requirements. Every version is assigned a number within the JNL system. For example, a JTIDS network library designed as a primary air defense datalink will have increased bandwidth and transmission time for units possessing air surveillance radars and increased priority for the transmission of return tracks from interceptors to controlling units.

On the other hand, a ground-centric JNL, where air superiority has been achieved, will trade air defense priorities for increased ground unit participation with an accompanying shift in bandwidth availability. Keep in mind that compatibility between different JNLs is possible, with smaller "nodes" being established within the entire network. In addition to being network specific, the JNLs also use software specific to the participating platform.

While it may be an oversimplification to say that the United Kingdom uses the JTIDS as its primary air traffic control network, it is accurate to say that it plays a major role in providing big-picture oversight regarding flight safety and national defense. As a result, JTIDS operations

in the U.K. are highly regulated by the JDLMO, and non-compliance with procedures results in expulsion from the network. In fact, prior to conducting any link operation in the U.K., a platform must be granted permission to operate by the U.K. Civil Aviation Authority.

The architecture of JTIDS in the U.K. is similar to that of a U.S. Navy carrier strike group with network time reference (NTR), a highly accurate system time used to coordinate transmission and receive times, held by remote terminal modules (RTMs). Participants contributed either through direct contact with the remote terminal module or through units acting as relays or data forwarders.

By direction of the JDLMO, surface combatants used airborne assets as "air bridges" to provide an extended line of sight. These air bridges consisted primarily of the E-3D airborne warning and control system (AWACS) and E-2C Hawkeye aircraft, but any Multifunctional Information Distribution System (MIDS) capable aircraft can provide the relay needed for entry and full participation in the network.

The JNL specifically constructed for Saxon Warrior met all of the information exchange requirements of the participating units, but also remained within the constraints of the U.K. Frequency Clearance Agreement, as well as the operating restrictions of the U.K.'s tactical datalink (TDL) policy.

The Saxon Warrior JTIDS network library and platform specific loads were released for U.S. assets in the weeks preceding the exercise, but arrived too late to be included in a scheduled link exercise prior to mobilization. As a result, the first operational trials between U.S. units occurred during the trans-Atlantic voyage; no interoperability tests took place until arrival in the exercise area.

Tests between U.S. forces were marginally successful, with the USS George H. W. Bush (GHWB) acting as the network time reference node. Test metrics were measured through Fine Sync indications at individual terminals and the successful transmission and receipt of precise participant location and identification (PPLI) symbols and JTIDS voice communications (J-Voice).

Although all participants received hardware indications that synchronization was achieved, no consistent level of communications existed between units. In the E-2C, hardware indications of Coarse Sync were displayed without PPLI symbols, but two-way voice communications were possible using the voice circuit. This condition was contrary to the system knowledge possessed by the typical crew member. Additionally, where hardware indications showed Fine Sync, voice communications were not possible even while PPLI symbols were present.

Exercise Operations

Line-of-sight considerations because of range prevented direct entry of surface assets into the U.K.'s link architecture. To maintain a recognized air and maritime picture, the aircraft carrier assumed the role of the network time reference node

GULF OF OMAN (March 25, 2009) An E 2C Hawkeye, assigned to the "Bear Aces" of Carrier Airborne Early Warning Squadron (VAW) 124 flies over the Gulf of Oman. U.S. Navy photo by Mass Communication Specialist 3rd Class Jonathan Snyder.

when airborne assets were not available. Without line of sight to the RTMs, this surface node was able to operate independently in several operating areas without interfering with frequencies used by shore-based facilities.

Upon commencement of flight operations, the intent was for the E-2C Hawkeye to establish itself in the link with the shore remote terminal module at Tregantle Fort in southeast Cornwall. GHWB relinquished its role as the NTR and entered the U.K. datalink architecture via the relay option incorporated in the Hawkeye's software load.

As MIDS aircraft would launch, the connectivity between the GHWB and remote terminal module was further enhanced by virtue of the network configuration. The air bridge would allow the transfer of information as long as the E-2C could receive system time from the remote terminal module and transmit that system time to the GHWB.

With these two single points of failure and an untested interface between forces, the stage was set for troubleshooting over several variables and operating conditions. Of note, it was discovered only during the last few days of the exercise that one of the four E-2C aircraft was unable to transmit JTIDS data because of a damaged transmission line.

Another aircraft could not transmit because of a faulty control unit. The two aircraft were able to "passively" enter JTIDS, but did not relay any timing data or their own precise participant location and identification symbols.

Additionally, reliability issues with the RTM at Tregantle Fort prevented timely troubleshooting for the E-2C system's degradation.

Problems that arose during the first few days of Saxon Warrior led to the systematic analysis of various hardware and software configurations, as well as contact with SPAWARSYSCEN Pacific regarding the stability of the E-2C's JNL. While link connectivity was achieved between the carrier strike group and U.K., it was unreliable and did not provide a useful tactical picture.

Specifically, it was apparent that the E-2C was not relaying PPLIs from surface combatants to the U.K., and the carrier strike group did not receive any air tracks present in the U.K. datalink. After reviewing the parameters of the existing JTIDS network library, SPAWARSYSCEN Pacific released a revised version of the software, ensuring that a PPLI relay feature was entered and activated. This new software configuration proved moderately successful, and with the discovery of the faulty JTIDS equipment in the E-2C, link operations improved. However, with the end of the exercise near, limited data were collected to prove the validity of the new software build.

The incorporation of reliable very and ultra high frequency voice communications between the E-2C and ground stations is an absolute necessity.

Recommendations

The successful integration of non-organic nodes with pre-existing data architecture is the key component to any effective command, control, communications, computers and intelligence (C4I) structure. To achieve successful integration, two single points of failure were incorporated to bring the GHWB Strike Group into the U.K. datalink. Even under the most ideal situations, this is a risky proposition, and combined with a lack of reliable communications between shore facilities and the E-2C aircraft for troubleshooting indications on both sides of the links, there was little that could be done at the operator level.

The incorporation of reliable very and ultra high frequency voice communications between the E-2C and ground stations is an absolute necessity. Additionally, communications between the ground station command elements and remote equipment locations would greatly decrease the time needed to troubleshoot equipment and increase the time allotted to focus on software anomalies because of the limited endurance of the aircraft.

While the JDLMO liaison officer aboard GHWB proved invaluable in relaying information to the remote terminal module when UHF communications failed, the lack of sufficient operational evaluation of the JNL and common technical language between aircrew and ground operators did not contribute to the success of this operation. Overall, the successful execution of this exercise was generally achieved in spite of, rather than because of the quality of the datalink. While conducting large force operations, U.S. forces usually create a standalone datalink for their own operating area, with minimal interaction with CONUS shore-based facilities required. In the U.K. operational environment, this is not an option because of the strict regulation of Link 16 operations. To improve the performance of JTIDS during joint exercises, prior planning, combined with dedicated troubleshooting, are two simple solutions to the problems encountered during Saxon Warrior.

While an embarked JDLMO liaison officer greatly helped with the integration of carrier strike group assets with the U.K. datalink structure, on-site representatives from the strike group were not present at any of the remote terminal module nodes or any other ground stations. Specifically, a representative from the E-2C squadron familiar with the operation of JTIDS would have provided the real-time assessment needed for various troubleshooting steps that are unique to the E-2C, and the common technical language that was lacking could have been mitigated through this liaison officer.

Prior to the commencement of the exercise, operational testing should be performed through the use of an actual E-2C to gauge the compatibility of the software load. The role of the liaison officer would be integral to this phase as well, providing specific technical characteristics which would aid in the resolution of any problems that might arise.

Attendance and participation of a liaison at the initial planning conferences and through the execution phase would provide a single point of contact and technical expertise to bridge the gap between the strike group and allied forces.

Optimally, these recommended solutions would contribute to the overall success of JTIDS operations. If this is not feasible, even implementing one of the recommendations would pay great dividends toward improving interoperability between systems and foster the spirit of cooperation necessary to the success of any allied operation. CHIPS

Lt. Dennis A. Szpara is an E-2C naval flight officer with the VAW-124 "Bear Aces."

A Communications Planning Primer

What every "commo" needs to know

By Capt. Danelle Barrett

Lt. Cmdr. Ima Eyep, a recent information professional lateral transfer from the surface warfare community, checks aboard a strike group as the communications officer, or "commo." Within two weeks of moving into her new job, an earthquake hits in the Caribbean and Eyep's strike group is assigned as the combined forces maritime component commander, or CFMCC, to manage naval humanitarian assistance and disaster relief (HA/DR) efforts for two countries located on different islands affected by the catastrophe.

It is unknown at the onset of the operation which forces will participate or if branch and sequel plans will be needed for potential peacekeeping functions, non-combatant evacuation operations or maritime intercept operations should the situation on the ground take a turn for the worse.

Eyep's new boss looks to her to quickly get the communications plan released to enable command and control (C2) of multinational forces. She does not have previous communications planning experience or training. However, she has an experienced senior chief information systems technician assigned as the strike group spectrum manager. They have 48 hours to get the communications plan out via naval message. Failure to plan and execute a robust communications plan will equate to uncoordinated C2 for the CFMCC forces, ineffective response and, most likely, loss of life. The clock is ticking.

This scenario could become reality for any commo today. The biggest challenge is that most commos have little or no experience in actual communications planning when they arrive on assignment. Additionally, there is no formal Navy training available regarding communications planning for tactical and operational scenarios so most commos credit the school of hard knocks as their training ground. Although the Afloat Electromagnetic Spectrum Operations Program (AESOP) is an effective spectrum management software tool for managing radar and communications frequencies for shipboard equipment, and training is available through the Naval Surface Warfare Center Dahlgren Division, the wider framework for communications planning is not covered.

Avoiding the School of Hard Knocks

While the Navy needs formalized long-term instruction for commos, as an interim step, there are certain basic communications planning concepts that can be followed to prepare communications officers to meet this challenge. This primer provides commos with fundamentals to consider when developing communications plans to support operations, as well as suggestions to avoid common missteps. Key tenets of the communications planning framework, regardless of type of operation, include the following lessons learned.

As commo, invite yourself to the planning party — be active in all operational planning meetings and ensure participants understand and include potential communications implications or limitations in their plans. Commos should be so involved in planning that operators would not even consider having a planning session without the commo present.

Understand the commander's C2 structure and its implications to command, control, communications and computers (C4) planning and operations.

Know the commander's critical information requirements (CCIRs) and those of the commander's boss.

Know the mission. Understanding the mission will help anticipate communications and C2 requirements in advance.

Identify C4 requirements. Coordinate with operators and others to gather requirements early and get their buy-in for the plan prior to release. Give the commander some C4 maneuver space whenever possible.

Remember, based on the scenario, there may be unique C4 requirements to consider. For example, non-combatant evacuation and repatriation operations will involve heavy use of ship-to-shore communications with Marine ground units, and operational tasking order communications (OPTASK COMMS) need to be aligned with the larger joint task force (JTF) plan.

HA/DR operations may involve communications with non-governmental organizations (NGOs) and interagency groups, like the U.S. Department of State and United States Agency for International Development (USAID). Internal response in the United States will also include communications with state and municipal local first responders. The commo cannot assume interoperability between all the players and their systems.

For any operation, consider where tactical ground units will be ashore and the issues that may be encountered, for example, electromagnetic interference, antenna look angles, foreign frequency landing rights, etc.

In combat operations, communications may be denied by adversaries' actions. Planning for redundancy and communications discipline is key.

Plan for the unknown. Build in additional capacity for potential branch and sequel plans and make the communications plan releasable to the widest audience possible from the onset. This will enable the plan to flex as operations change and allow effective participation by multinational partners.

Coordinate early with asset providers to provide maximum coverage across the frequency spectrum using all available C4 systems.

Know the communications capabilities and limitations of units assigned and those of anticipated participants.

Ensure the plan is aligned and in support of operational orders (Annex K for Communications and Annex C for Operations) from higher authority and strike group operational tasking orders for information and knowledge management, link, information warfare and intelligence.

Ensure maritime planners are in lockstep with joint planners coordinating spectrum use and assets in support of

operations. This includes spectrum use by surface, air and subsurface unmanned vehicles.

Plan for communications failure. Build in sufficient redundancy to ensure continuous C2.

An effective communications planner builds a comprehensive communications architecture with sufficient redundancy and robustness to deftly support the commander's ability to seamlessly execute command and control. Getting the architecture and plan in place is not without challenges.

Understanding the C4 Requirements — Communications "Fairyland" versus Communications Reality

In all communications planning, the first step is to determine the operational requirements that need to be supported. This is where communications fairyland meets communications reality. In communications fairyland, operators understand the mission fully, know their C2 structure and understand the geography of the operation, the enemy and friendly forces at their disposal. They assume a flawless communications environment and perfect systems performance.

The reality at the onset of a crisis is operators, as well as commos, will need answers to a multitude of planning questions, and the structures will not be mature enough for many of the critical factors to be known. Communications planners must do their best to build sufficient capacity into the communications architecture to support what operators have identified definitively and to anticipate what might become important in later phases of the operation.

When planning the best C2 structure with operators, it is important to determine the commander's role. Will he or she be the coalition/joint task force commander, the JFMCC commander, an expeditionary strike force (ESF) commander, task group commander, etc.?

Understanding the commander's role, and if that role is likely to change, will be key for developing the correct type of officer in tactical command (OTC) and composite warfare commander (CWC) structure and corresponding communications plan.

For example, if the C2 structure is for an ESF and a SUBSIT A C2 structure is chosen, there are communications implications that come into play. SUBSIT A is essentially a flat organization structure where all warfare commanders and their subordinate units report to the ESF commander on the same voice and data nets, to include chat rooms. Depending on the number of participants, these nets could get very busy and cause delays in delivery and receipt of operational orders.

In a SUPSIT B, the composite warfare commanders report to the expeditionary strike group commander on ESF command nets but have separate voice and data nets for use between them and their subordinate units. Communications factors, such as a unit's equipment capabilities and limitations, as well as the number of participants and where units are located, must be taken into account when making decisions on which C2 structure to implement to meet operational objectives.

It is important for operations personnel to get operational orders, task unit (TU) and task group (TG) assignments out early. During a crisis, the situation is rapidly evolving so communications planners should not wait to get the first communications plan out while waiting for final TU/TG assignments.

The initial plan should be issued with an 80 percent solution to get the structure in place to immediately begin command and control; the plan can be amended as units are added or removed. Special attention to subordinate groups and units that often implement their own communications plans, such as Marine expeditionary units, carrier air wings and Special Forces, must be known by higher level communications planners to ensure alignment and deconfliction of frequencies.

Understanding Implications of C4 Capabilities and Limitations

The communications planner's attendance at all operational planning discussions is paramount to ensuring that communications asset availability and unit limitations are well thought out when determining the C2 structure. While operators will say that communications do not drive operations, in reality, that is indeed true in many cases.

For example, maritime forces are extremely dependent on satellites for communications between units separated by more than 200 nautical miles. Selecting a C2 structure with disaggregated forces all using high frequency (HF) or line of sight (LOS) for the commander's primary voice nets is unsupportable. If satellite assets are unavailable or limited, operators must decide on a C2 structure that accounts for these factors, and a SUPSIT B structure is more appropriate. Also, planners must acknowledge these assets are largely joint assets and not strictly Navy resources.

Communications planners also need to be mindful of joint, coalition and interagency unit communications capabilities.

Communications planners also need to be mindful of joint, coalition and interagency unit communications capabilities. Use of these capabilities should be included in the overall plan to avoid interoperability issues or frequency interference problems. In a JTF environment, this could include special warfare units, elements of the Joint Communications Support Element, and other service, interagency or coalition unique communications platforms.

Many coalition units do not share common satellite systems or cryptographic equipment with the United States, so how operational orders will be passed to them must be built into communications and communications security planning.

Communications planners should aggressively work with satellite service providers to put as many of their assigned voice and data command nets on the same satellite for smaller units that do not have the capability to be on more than one satellite simultaneously due to equipment limitations shipboard.

Where communications problems exist, due to unit equipment limitations, casualties or lack of satellite access, operators who "own" the voice/data net (the net controlling station or NECOS) should assign a guard ship to help relay operational orders to those disadvantaged units. The guard ship relationships should be codified in the OPTASK COMMS to ensure continuous C2 is achieved.

For bandwidth disadvantaged units, afloat and ashore, special consideration should be given by planners when using

websites as a primary means of information dissemination, particularly C2 information. The Army and Air Force rarely use traditional message traffic for disseminating operational orders and post most orders to websites. However, the Navy and many coalition partners still use message traffic due to bandwidth limitations afloat which make Web-based collaborative tools challenging or impossible to use while underway. Annex C to the operational order and the OPTASK for knowledge and information management must account for these variations.

The second and third order effects of using collaborative or Web-based tools should be included in communications planning. For example, do units have access to high data rate Internet Protocol communications? Do fleet firewall ports and protocols support use of the tool? Is the tool or website bandwidth efficient and usable afloat? Do afloat units have the software or Web plug-ins approved for shipboard use? Do Navy units have to implement bandwidth management measures to meet the requirements?

Navy commanders' assigned roles and where they physically reside during operations will have an impact on how they can effectively communicate with superiors and subordinates. For example, having the combined forces maritime component commander collocated with the JTF commander, specifically at a shore location with robust connectivity, eliminates the challenges of communicating with the boss although those challenges will remain in communicating with subordinates on the tactical edge.

Mitigation measures can be put in place, such as having the CFMCC push only required information to subordinate units via Collaboration at Sea or other bandwidth efficient tools, and ensuring sufficient redundancy for voice and data nets between the commander ashore and subordinate units afloat to allow for redundancy to pass operational orders.

When Web-based tools, including social networking sites, are able to be used they should be leveraged by communications and operational planners for their tactical advantages, particularly during unclassified operations — like HA/DR efforts. For example, communications planners could use Twitter to discern if commercial connectivity to an area is still operational. If the affected population is "tweeting" — commercial communications are available. This is important because where terrestrial and wireless commercial infrastructure communications can be leveraged, less military or temporary tactical commercial satellite terminals are needed for ground units.

Operations personnel can also use the tools to gain more real-time, albeit not analyzed, situational awareness of events happening on the ground where there is not yet a military presence.

Plan for Communications Failure

Taking into account all the factors discussed, a commo must plan for communications failure and have alternatives available when there is a disruption in primary communications paths and still be able to maintain command and control. Because of the Navy's overreliance on satellite service to reach-back ashore for high data rate communications, planners must be ready for operating in a satellite-denied environment due to equipment casualties, insufficient shared satellite capacity, or enemy disruption to communications links or space-based services.

A commo does this through the optimum C2 organizational structure with redundant communications paths via various systems using different bands of the radio frequency spectrum.

Working closely with a spectrum manager, a commo should build a communications plan that includes multiple paths for key C2 circuits using multiple portions of the spectrum. The spectrum manager coordinates with the Navy and Marine Corps Spectrum Center to obtain high, ultra high and very high frequency spectrum for use in the communications plan.

Spectrum managers also work with numbered fleet commanders to request satellite-based assets for voice and data nets via various systems. Prioritization of the multiple circuits is included in the plan. To remove ambiguity for operators and time permitting, the various paths should be tested with participating units in advance to ensure agility in execution.

Conscientious communications planners will also review the Navy and Joint Lessons Learned databases to discover potential pitfalls and avoid those early. Too often, the wheel is reinvented and lessons unnecessarily and painfully relearned. By the same token, at the end of operations, commos should enter their hard lessons learned into the Navy and Joint Lessons Learned databases to help shipmates prepare for similar operations.

Best Practices, Careful Planning and Working Together Yield Success

So we return to Eyep and her challenge. Working with the strike group's spectrum manager, she quickly researched lessons learned from previous HA/DR efforts and discerned best practices. She synchronized internally with strike group operations, and intelligence and logistics subject matter experts to obtain their best assessment of communications requirements and units participating — along with their capabilities and limitations.

Eyep coordinated with the joint task force J6 communications planners to understand requirements for information exchange with the JTF commander. She gave critical recommendations on communications factors which will affect decisions regarding which C2 structure will be ultimately selected by the commander.

Then Eyep creatively built a plan that included redundant circuits, paths and systems using all available assets to ensure continuous C2 between the commander and his or her forces. She included circuits in her plan that cover scenarios for potential branches and sequels deviating from the main plan and made the communications plan releasable to as many coalition partners as possible.

Eyep's coordination with the joint task force knowledge manager paid big dividends because she ensured the KM understood the communications limitations of maritime bandwidth disadvantaged units and included effective means to exchange information with those forces.

Finally, Eyep knows the plan is a first iteration and that it will evolve as operations change. She remains actively engaged in all aspects of operations, looking for the next opportunity to improve C2. CHIPS

Capt. Danelle Barrett is an Information Dominance Corps officer with 22 years of experience in communications. She has led communications planning efforts during four carrier strike group and numbered fleet commander staff tours. Barrett is the commanding officer of Naval Computer and Telecommunications Area Master Station Atlantic.

Q&A with Senior Chief Information Systems Technician Jason M. Rufa — Carrier Strike Group Two Spectrum Manager

Capt. Danelle Barrett, an information professional officer and commanding officer of Naval Computer and Telecommunications Area Master Station Atlantic, interviewed ITCS Rufa in March 2011.

Q: Tell us about your job as the strike group spectrum manager. How did the Navy prepare you to be an afloat spectrum manager?

A: I did three-and-a-half months of spectrum management school [Electromagnetic Spectrum Management Course] at Keesler Air Force Base, Biloxi, Miss. Training was very informative, but there is nothing like fleet experience. Being thrown in the middle of a carrier strike group deployment is the best training any spectrum manager can receive. When you're deployed, it's either sink or swim, and we do not have the option of sinking.

Operation Unified Response, JTF (Joint Task Force) Haiti, was another opportunity to train/operate. On short notice, we put together the USS Carl Vinson Carrier Strike Group, USS Bataan Amphibious Readiness Group (ARG) and USS Nassau ARG communication plan. Again, in conjunction with NMCSO LANT (Navy Marine Corps Spectrum Office Atlantic), Marine Corps and U.S. SOUTHCOM (U.S. Southern Command) spectrum managers, we put together and then deconflicted a rather lengthy communications plan.

Q: Who do you work with outside the strike group for managing the frequency spectrum?

A. We have worked with Navy and Marine Corps Spectrum Offices: NMCSO LANT, NMCSO Europe [in Naples, Italy], NMCSO Central Command [in Bahrain], Commander, Naval Network Warfare Command and fleet/COCOM (combatant commander) spectrum managers.

Q: What are the biggest challenges you face in managing the spectrum for strike group operations?

A: Multiple CSGs and/or ARGs operating in the same area at the same time with multiple frequency requirements and a limited amount of available spectrum.

Q: Are there differences in how you manage frequencies during training and when deployed?

A: We train like we fight. During the recent Group Sail [Jan. 19-Feb. 23, 2011] and COMPTUEX/JTFX (Composite Unit Training Exercise/Joint Task Force Exercise) for USS George H. W. Bush Carrier Strike Group, we had limited frequencies because of being underway at the same location with the Enterprise Carrier Strike Group. We worked hand-in-hand with our Enterprise Carrier Strike Group and NMCSO LANT counterparts to deconflict spectrum issues as we would in a deployed environment.

Q: You were the lead spectrum manager afloat during Operation Unified Response in Haiti. What were some of the unique challenges you faced afloat and ashore in managing frequencies during that situation? Did you have to work with different organizations in the JTF environment to manage frequencies?

A: Some of the challenges came from commander and unit specific requirements. As a humanitarian assistance operation, requirements are different than a typical carrier strike group deployment. Also, frequency request procedures were a bit of a challenge. The procedures for requests in a joint environment are slightly different than what we were used to. We worked hand-in-hand with the Army, Marine Corps and Air Force to manage frequencies.

Q: What are some of the changes you have seen in the last two years in how the Navy manages frequencies afloat? What changes do you see coming?

A: Moving from creating a unit specific frequency plan to predesignated communication plans. The changes I see include having a more restricted operating environment with less frequencies available for use.

ITCS Jason Rufa aboard USS Theodore Roosevelt (CVN 71).

Q: What advice would you give to more junior information systems technicians who would like to be a spectrum manager some day?

A: I would say don't just look at the OPTASK COMM (operational tasking communications) [planner] for a frequency. Understand all sections of it, from emission designators, down to the guard requirements. Familiarize yourself with AESOP (Afloat Electromagnetic Spectrum Operations Program) and your ship's communication capabilities. There are dozens of resources available on NKO (Navy Knowledge Online) and SIPRNET. All you have to do is look.

Take a tour of your local Navy and Marine Corps Spectrum Office. These are the subject matter experts. They are the professionals who supply the fleet with all our spectrum needs. CHIPS

The Navy and Marine Corps Spectrum Center and offices (NMSC) are the Department of the Navy activities responsible to ensure compliance with international, national, and Department of Defense electromagnetic spectrum management policies and regulations.

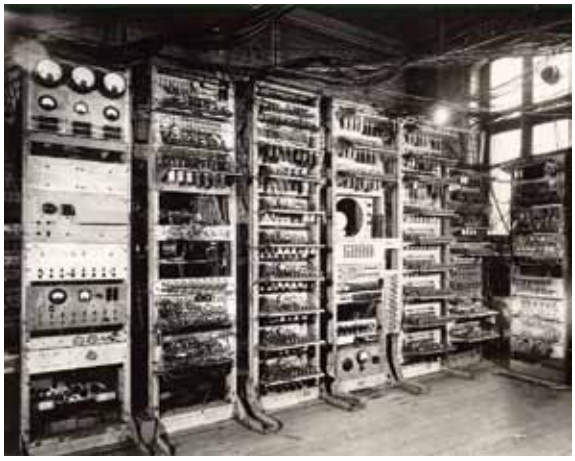
They are uniquely qualified to represent the electromagnetic spectrum policy interests of the DON, and are the Navy's primary organizations responsible for implementation of electromagnetic spectrum policy.

"Amazing Grace"

A pioneer in programming languages and technology development, Rear Adm. Grace Hopper was instrumental in bringing computer technology to Navy desktops and individuals. Hopper had an uncanny ability to predict the IT trends of the future. Many of her predictions came true during her lifetime as industry built more powerful, more compact machines. Some of her more innovative ideas included using computers for predicting weather patterns and ocean waves, tracking the life cycle of crop eating locusts, and managing water reserves. In 1986, President Ronald Reagan awarded Hopper the prestigious National Medal of Technology at a ceremony in the White House. But Hopper considered her highest award to have been "the privilege and honor of serving very proudly in the United States Navy."

Lt. j.g. Grace Brewster Hopper (seated second from right) with Cmdr. Howard H. Aiken (seated center), who developed the first large scale digital computer, officially called the IBM automatic sequence controlled calculator, more commonly called the Harvard Mark I. The posed photograph, with other members of the Bureau of Ordnance Computation Project, was taken in front of the Mark I computer. Hopper started as the first programmer in 1944 on the Mark I (IBM ASCC). As a programmer, she used the Mark I to compute firing tables for weapons and then wrote them into a series of instructions for the computer. In 1946 she published a book, "A Manual of Operations for the Automatic Sequence Controlled Calculator." Hopper continued to work on the Mark II and Mark III. Photo taken at Harvard University, Cambridge, Mass., January 1944. Photo courtesy of Defense Visual Information Center.

Lt. j.g. Grace Brewster Hopper working at the Bureau of Ordnance Computation Project, Harvard University, Cambridge, Mass., January 1946. Photo courtesy of the Defense Visual Information Center. For more information about Hopper, visit the Naval History and Heritage Command website at www.history.navy.mil and search under "Grace Hopper."



The Mark I. Photo courtesy of the Computer Science Department of Virginia Polytechnic Institute and State University.

The Mark I – the impressive beast

The Mark I, programmed by pre-punched paper tape, could perform addition, subtraction, multiplication, division and reference to previous results. It had special subroutines for logarithms and trigonometry and used 23 decimal place numbers. Data was stored and counted mechanically using 3,000 storage wheels, 1,400 rotary dial switches and 500 miles of wire. Because of its electromagnetic relays it was considered a relay computer.

Output was displayed on an electric typewriter. The Mark I took three to five seconds to calculate a multiplication equation. It weighed five tons and contained almost 760,000 separate pieces. Lt. j.g. Grace Brewster Hopper was enchanted with its performance, until the UNIVAC I came along — operating a thousand times faster. The Navy used the Mark I until 1959.

As a child growing up in New York City, Hopper was "good with gadgets." When Hopper first saw the Mark I, she couldn't wait to start taking it apart to see how it worked. Remarking on the Mark I, Hopper said, "That was an impressive beast. She was fifty-one feet long, eight feet high and five feet deep."

Enterprise Software Agreements

The **Enterprise Software Initiative (ESI)** is a Department of Defense (DoD) initiative to streamline the acquisition process and provide best-priced, standards-compliant information technology (IT). The ESI is a business discipline used to coordinate multiple IT investments and leverage the buying power of the government for commercial IT products and services. By consolidating IT requirements and negotiating Enterprise Agreements with software vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in IT acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute and manage IT from the enterprise level.

Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 5000.2 on May 12, 2003.

Unless otherwise stated authorized ESI users include all DoD components, and their employees including Reserve component (Guard and Reserve), and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA, nor other IC employees, unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI website at www.esi.mil/.

Software Categories for ESI:

Asset Discovery Tools

Belarc

BelManage Asset Management – Provides software, maintenance and services.

Contractor: ***Belarc Inc.*** (W91QUZ-07-A-0005)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 28 Mar 12

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

BMC

Remedy Asset Management – Provides software, maintenance and services.

Contractor: ***BMC Software Inc.*** (W91QUZ-07-A-0006)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 23 Mar 15

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Carahsoft

Opsware Asset Management – Provides software, maintenance and services.

Contractor: ***Carahsoft Inc.*** (W91QUZ-07-A-0004)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 17 Sep 12

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

DLT

BDNA Asset Management – Provides asset management software, maintenance and services.

Contractor: ***DLT Solutions Inc.*** (W91QUZ-07-A-0002)

Authorized Users: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 01 Apr 13

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 37.

Oracle (DEAL-O)

Oracle Products – Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact the Navy project manager on page 38.

Contractors:

Oracle America Inc. (W91QUZ-07-A-0001); (703) 364-3110

DLT Solutions (W91QUZ-06-A-0002); (703) 708-8979

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0628

Mythics, Inc. (W91QUZ-06-A-0003); Small Business; (757) 284-6570

Affigent, LLC (W91QUZ-09-A-0001); Small Business; (571) 323-5584

Ordering Expires:

Oracle: 28 Mar 12
DLT: 01 Apr 13
immixTechnology: 02 Mar 16
Mythics: 18 Dec 11 (Please call for extension information.)
TKCIS: 9 Nov 11 (Please call for extension information.)

Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Special Note to Navy Users: See the information provided on page 38 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

Sybase Products – Offers a full suite of software solutions designed to assist customers in achieving Information Liquidity. These solutions are focused on data management and integration; application

www.esi.mil

integration; Anywhere integration; and vertical process integration, development and management. Specific products include but are not limited to: Sybase's Enterprise Application Server; Mobile and Embedded databases; m-Business Studio; HIPAA (Health Insurance Portability and Accountability Act) and Patriot Act Compliance; PowerBuilder; and a wide range of application adaptors. In addition, a Golden Disk for the Adaptive Server Enterprise (ASE) product is part of the agreement. The Enterprise portion of the BPA offers NT servers, NT seats, Unix servers, Unix seats, Linux servers and Linux seats. Software purchased under this BPA has a perpetual software license. The BPA also has exceptional pricing for other Sybase options. The savings to the government is 64 percent off GSA prices.

Contractor: ***Sybase, Inc.*** (DAAB15-99-A-1003); (800) 879-2273; (301) 896-1661

Ordering Expires: 15 Jan 13

Authorized Users: Authorized users include personnel and employees of the DoD, Reserve components (Guard and Reserve), U.S. Coast Guard when mobilized with, or attached to the DoD and nonappropriated funds instrumentalities. Also included are Intelligence Communities, including all DoD Intel Information Systems (DoDIIS) member organizations and employees. Contractors of the DoD may use this agreement to license software for performance of work on DoD projects.

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Application Integration

Sun Software

Sun Products – Provides Sun Java Enterprise System (JES) and Sun StarOffice. Sun JES products supply integration and service oriented architecture (SOA) software including: Identity Management Suite; Communications Suite; Availability Suite; Web Infrastructure Suite; MySQL; xVM and Role Manager. Sun StarOffice supplies a full-featured office productivity suite.

Contractors:

Commercial Data Systems, Inc. (N00104-08-A-ZF38); Small Business; (619) 569-9373

Dynamic Systems, Inc. (N00104-08-A-ZF40); Small Business; (801) 444-0008

Ordering Expires: 24 Sep 12

Web Links:

Sun Products
www.esi.mil/agreements.aspx?id=160
Commercial Data
www.esi.mil/contentview.aspx?id=160&type=2
Dynamic Systems
www.esi.mil/contentview.aspx?id=162&type=2

Enterprise Architecture Tools

IBM Software Products

IBM Software Products – Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA pricing. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products, including: IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

Contractor: ***immixTechnology, Inc.*** (DABL01-03-A-1006); Small Business; (703) 752-0641 or (703) 752-0646

Ordering Expires: 02 Mar 16

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

VMware

VMware – Provides VMware software and other products and services. This BPA has been designated as a GSA SmartBUY.

Contractor: ***Carahsoft Inc.*** (W91QUZ-09-A-0003)

Authorized Users: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 27 Mar 14

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS2)

Computer Associates Unicenter Enterprise Management Software – Includes Security Management; Network Management; Event Management; Output Management; Storage Management; Performance Management; Problem Management; Software Delivery; and Asset Management. In addition to these products, there are many optional products, services and training available.

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002); (703) 709-4610

Ordering Expires: 22 Sep 12

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Microsoft Premier Support Services (MPS-2)

Microsoft Premier Support Services – Provides premier support packages to small and large-size organizations. The products include Technical Account Managers, Alliance Support Teams, Reactive Incidents, on-site support, Technet and MSDN subscriptions.

Contractor: ***Microsoft*** (W91QUZ-09-D-0038); (980) 776-8413

Ordering Expires: 31 Mar 12

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

NetIQ

NetIQ – Provides Net IQ systems management, security management and Web analytics solutions. Products include: AppManager; AppAnalyzer; Mail Marshal; Web Marshal; Vivinet voice and video products; and Vigilant Security and Management products. Discounts are 8 to 10 percent off GSA schedule pricing for products and 5 percent off GSA schedule pricing for maintenance.

Contractors:

NetIQ Corp. (W91QUZ-04-A-0003)

Northrop Grumman – authorized reseller

Federal Technology Solutions, Inc. – authorized reseller

Ordering Expires: 05 May 14

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Quest Products

Quest Products – Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. Only Active Directory products have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.

Contractors:

Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4889

DLT Solutions (W91QUZ-06-A-0004); (703) 708-9127
Ordering Expires:
Quest: 29 Dec 15
DLT: 01 Apr 13
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Resource Planning

Oracle

Oracle – *See information provided under Database Management Tools on page 34.*

RWD Technologies

RWD Technologies – Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.
Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (404) 845-3624
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: www.esi.mil/contentview.aspx?id=150&type=2

SAP

SAP Products – Provide software licenses, software maintenance support, information technology professional services and software training services.
Contractors:
SAP Public Services, Inc. (N00104-08-A-ZF41);
Large Business; (202) 312-3515
Advantaged Solutions, Inc. (N00104-08-A-ZF42);
Small Business; (202) 204-3083
Carahsoft Technology Corporation (N00104-08-A-ZF43);
Small Business; (703) 871-8583
Oakland Consulting Group (N00104-08-A-ZF44);
Small Business; (301) 577-4111
Ordering Expires: 14 Sep 13
Web Links:
SAP – www.esi.mil/contentview.aspx?id=154&type=2
Advantaged – www.esi.mil/contentview.aspx?id=155&type=2
Carahsoft – www.esi.mil/contentview.aspx?id=156&type=2
Oakland – www.esi.mil/contentview.aspx?id=157&type=2

Information Assurance Tools

Data at Rest (DAR) BPAs offered through ESI/SmartBUY

The Office of Management and Budget, Defense Department and General Services Administration awarded multiple contracts for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices.

These competitively awarded BPAs provide three categories of software and hardware encryption products — full disk encryption (FDE), file encryption (FES) and integrated FDE/FES products to include approved U.S. thumb drives. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

Licenses are transferable within a federal agency and include secondary use rights. All awarded BPA prices are as low as or lower than the prices each vendor has available on GSA schedules. The federal government anticipates significant savings through these BPAs. The BPAs were awarded under both the DoD's Enterprise Software Initiative (ESI) and GSA's governmentwide SmartBUY programs, making them available to all U.S. executive agencies, independent establishments, DoD components, NATO, state and local agencies, Foreign Military Sales (FMS) with written authorization, and contractors authorized to order in accordance with the FAR Part 51.

Service component chief information officers (CIO) are developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution.

The Department of the Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHESS website at https://chess.army.mil/ascp/commerce/index.jsp. As of this printing, the Air Force has not yet provided a DAR solution.

immix Group, *Inc.* (FA8771-07-A-0301)
McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)
Information Security Corp. – ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)
McAfee – ***Spectrum Systems, Inc.*** (FA8771-07-A-0304)
SafeNet, Inc. – ***SafeNet, Inc.*** (FA8771-07-A-0305)
Checkpoint – ***immix Group, Inc.*** (FA8771-07-A-0307)
SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)
WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)
CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)
Symantec, formerly GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)
Ordering Expires: 14 Jun 12 (If extended by option exercise.)
Web Link: www.esi.mil

Websense (WFT)

Websense – Provides software and maintenance for Web filtering products.
Contractor: ***Patriot Technologies*** (W91QUZ-06-A-0005)
Authorized Users: This BPA is open for ordering by all DoD components and authorized contractors.
Ordering Expires: 08 Sep 12
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Xacta

Xacta – Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.
Contractor: ***Telos Corp.*** (FA8771-09-A-0301); (703) 724-4555
Ordering Expires: 24 Sep 14
Web Link: https://esi.telos.com/contract/overview/default.cfm

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

iGrafx – Provides software licenses, maintenance and media for iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.
Contractors:
Softchoice Corporation (N00104-09-A-ZF34); (416) 588-9002 ext. 2072
Softmart, Inc. (N00104-09-A-ZF33); (610) 518-4192
SHI (N00104-09-A-ZF35); (732) 564-8333
Authorized Users: These BPAs are co-branded ESI/GSA SmartBUY BPAs and are open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community, authorized DoD contractors and all federal agencies.

Ordering Expires: 31 Jan 14

Web Links:
Softchoice
www.esi.mil/contentview.aspx?id=118&type=2
Softmart
www.esi.mil/contentview.aspx?id=117&type=2
SHI
www.esi.mil/contentview.aspx?id=123&type=2

Minitab

Minitab – Provides software licenses, media, training, technical services and maintenance for products, including: Minitab Statistical Software, Quality Companion and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***Minitab, Inc.*** (N00104-08-A-ZF30); (800) 448-3555 ext. 3256

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.

Ordering Expires: 07 May 13

Web Link: www.esi.mil/contentview.aspx?id=73&type=2

PowerSteering

PowerSteering – Provides software licenses (subscription and perpetual), media, training, technical services, maintenance, hosting and support for PowerSteering products: software as a service solutions to apply the proven discipline of project and portfolio management in IT, Lean Six Sigma, Project Management Office or any other project-intensive area and to improve strategy alignment, resource management, executive visibility and team productivity. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***immix Group, Inc.*** (N00104-08-A-ZF31);
Small Business; (703) 663-2702

Authorized Users: All DoD components, U.S. Coast Guard, NATO, Intelligence Community, and authorized DoD contractors.

Ordering Expires: 14 Aug 13

Web Link: www.esi.mil/contentview.aspx?id=145&type=2

Office Systems

Adobe Desktop Products

Adobe Desktop Products – Provides software licenses (new and upgrade) and maintenance for numerous Adobe desktop products, including Acrobat (Standard and Professional); Photoshop; InDesign; After Effects; Frame; Creative Suites; Illustrator; Flash Professional; Dreamweaver; ColdFusion and other Adobe desktop products.

Contractors:

Dell Marketing L.P. (N00104-08-A-ZF33); (312) 705-1889

CDW Government, LLC (N00104-08-A-ZF34); (301) 340-3402

GovConnection, Inc. (N00104-08-A-ZF35); (800) 862-8758

Insight Public Sector, Inc. (N00104-08-A-ZF36); (703) 871-8556

Ordering Expires: 30 Jun 12

Web Links:
Adobe Desktop Products
www.esi.mil/agreements.aspx?id=52
Dell
www.esi.mil/contentview.aspx?id=53&type=2
CDW-G
www.esi.mil/contentview.aspx?id=52&type=2
GovConnection
www.esi.mil/contentview.aspx?id=33&type=2
Insight
www.esi.mil/contentview.aspx?id=54&type=2

Adobe Server Products

Adobe Server Products – Provides software licenses (new and upgrade), maintenance, training and support for numerous Adobe server products including LiveCycle Forms; LiveCycle Reader Extensions; Acrobat Connect; Flex; ColdFusion Enterprise; Flash Media Server and other Adobe server products.

Contractor:

Carahsoft Technology Corp. (N00104-09-A-ZF31);
Small Business; (703) 871-8503

Ordering Expires: 14 Jan 14

Web Link: www.esi.mil/contentview.aspx?id=186&type=2

Microsoft Products

Microsoft Products – Provides licenses and software assurance for desktop configurations, servers and other products. In addition, any Microsoft product available on the GSA schedule can be added to the BPA.

Contractors:

CDW Government, LLC (N00104-02-A-ZE85); (888) 826-2394

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 7253702 or (512) 725-3702

GovConnection (N00104-10-A-ZF30); (301) 340-3412

GTSI (N00104-02-A-ZE79); (800) 999-GTSI ext. 2071

Hewlett-Packard (N00104-02-A-ZE80); (845) 337-6260

Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758

SHI (N00104-02-A-ZE86); (800) 527-6389 or (732) 564-8333

Softchoice (N00104-02-A-ZE81); (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

Ordering Expires: 31 Mar 13

Web Link: www.esi.mil/agreements.aspx?id=173

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI). The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server). August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA-approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager. The Red Hat products and services provided through the download site are for exclusive use in the following licensed community: (1) All components of the U.S. Department of Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DoD employees (e.g., contractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a Red Hat product to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the websites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the August Schell Red Hat download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the websites listed below for additional information to help you to make this determination before you obtain the software from the August Schell Red Hat download site (or contact the project manager).

GCSS users: Global Combat Support System
www.disa.mil/gcssj

Contractor: ***August Schell Enterprises*** (www.augustschell.com)
Download Site: http://redhat.augustschell.com
Ordering Expires: Nov 12; All downloads provided at no cost.
Web Link: www.disa.mil

Red Hat Linux

Red Hat Linux – Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractors:
Carahsoft Technology Corporation (HC1028-09-A-2004)
DLT Solutions, Inc. (HC1028-09-A-2003)
Ordering Expires:
Carahsoft: 09 Feb 14
DLT Solutions, Inc.: 17 Feb 14
Web Link: www.esi.mil

Sun (SSTEW)

SUN Support – Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)
Ordering Expires: 30 June 11 (Please call for information about follow-on contract.)
Project Management:
Jonnice Medley (301) 225-8081 (DSN 375) (jonnice.medley@disa.mil)
Web Link: www.disa.mil/contracts/guide/bpa/bpa_sun.html

Research and Advisory BPA

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via websites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded Dec. 1, 2006
Ordering Expires: Effective for term of GSA contract
Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.
Web Link: www.esi.mil/contentview.aspx?id=171&type=2

Autodesk

Autodesk – Provides software licenses for more than two dozen AutoCAD and Autodesk products.

Contractor: ***DLT Solutions*** (N00104-12-A-ZF30)
Ordering Expires: 20 Nov 14
Web Link: www.esi.mil/contentview.aspx?id=267&type=2

Department of the Navy Agreement

Oracle (DEAL-O) Database Enterprise License for the Navy

On Oct. 1, 2004 and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users, to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact Dan McMullan, NAVICP Mechanicsburg contracting officer, at (717) 605-5659 or email daniel.mcmullan@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific. The Navy Oracle Database Enterprise License provides significant benefits, including substantial cost avoidance for the department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:
a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

For your convenience all enterprise contract information is consolidated under

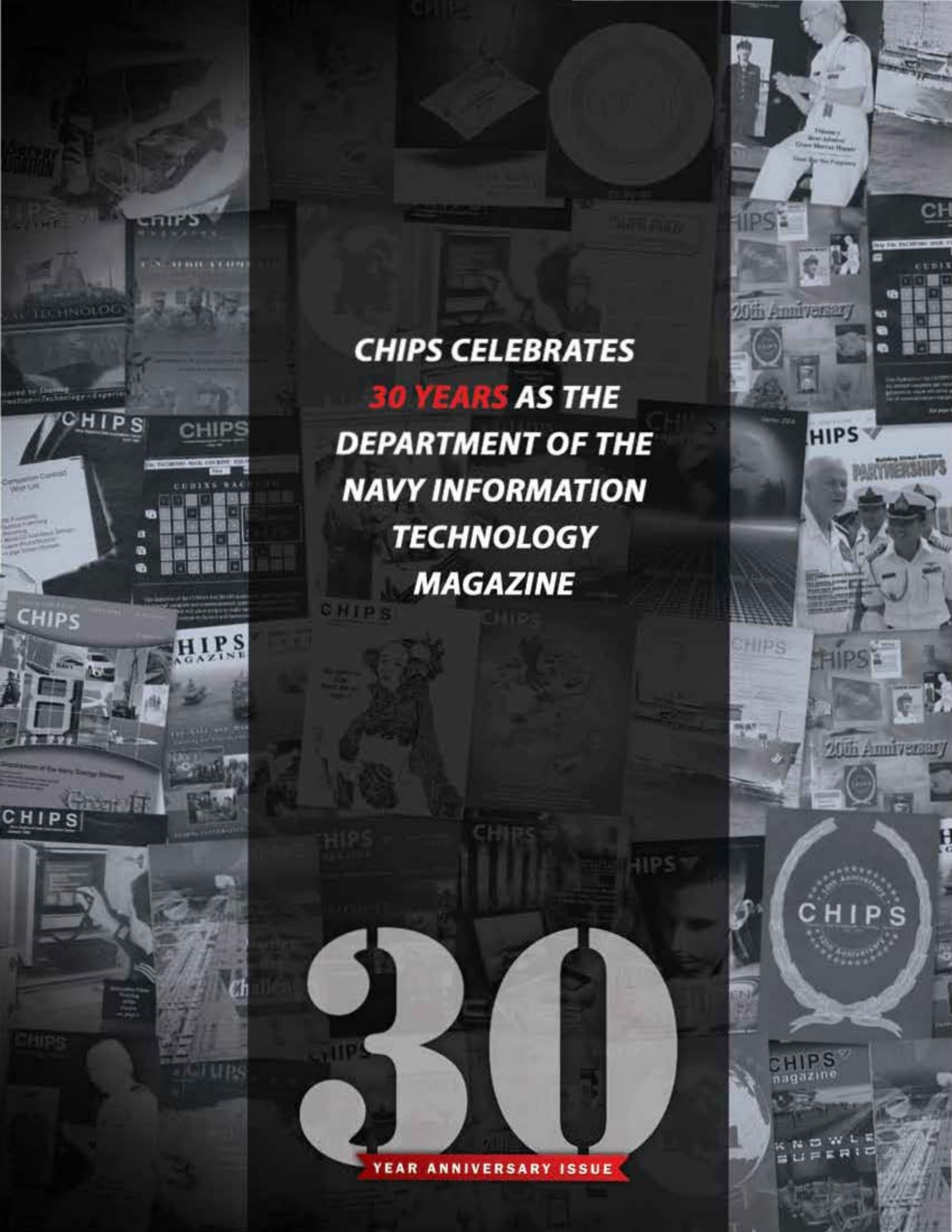
www.esi.mil

www.doncio.navy.mil/chips

www.doncio.navy.mil

ENTERPRISE COST $AVINGS ARE JUST A CLICK AWAY

VISIT OUR E-COMMERCE SITE - WWW.ITEC-DIRECT.NAVY.MIL


CHIPS CELEBRATES
30 YEARS AS THE
DEPARTMENT OF THE
NAVY INFORMATION
TECHNOLOGY
MAGAZINE
30
YEAR ANNIVERSARY ISSUE